

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 0 月 1 0 日
Date of Application:

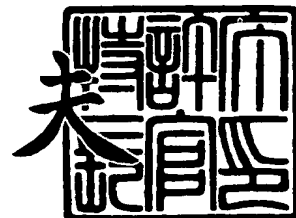
出 願 番 号 特 願 2 0 0 2 - 2 9 7 8 8 8
Application Number:
[ST. 10/C]: [J P 2 0 0 2 - 2 9 7 8 8 8]

出 願 人 株式会社リコー
Applicant(s):

2 0 0 3 年 7 月 1 8 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 0206950

【提出日】 平成14年10月10日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 G06F 12/00 537

【発明の名称】 セキュリティポリシーに基づいた文書の読み取り装置、
読み取り方法、ネットワーク配信を行う装置、ネットワ
ーク配信を行う方法及び、セキュリティポリシーを外部
から設定する入出力装置

【請求項の数】 76

【発明者】

【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内

【氏名】 斉藤 敦久

【発明者】

【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内

【氏名】 金井 洋一

【発明者】

【住所又は居所】 東京都大田区中馬込1丁目3番6号 株式会社リコー内

【氏名】 谷内田 益義

【特許出願人】

【識別番号】 000006747

【氏名又は名称】 株式会社リコー

【代理人】

【識別番号】 100070150

【弁理士】

【氏名又は名称】 伊東 忠彦

【先の出願に基づく優先権主張】

【出願番号】 特願2002-275973

【出願日】 平成14年 9月20日

【手数料の表示】

【予納台帳番号】 002989

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9911477

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 セキュリティポリシーに基づいた文書の読み取り装置、読み取り方法、ネットワーク配信を行う装置、ネットワーク配信を行う方法及び、セキュリティポリシーを外部から設定する入出力装置

【特許請求の範囲】

【請求項 1】 少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

を備えるセキュリティポリシーに基づいた文書の読み取り方法であって、

前記読み取り方法は、

前記ユーザ属性を取得するステップと、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得するステップと、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りが許可されているか否かを、前記セキュリティポリシーに基づいて判断するステップと、

前記読み取りが許可されていないと判断した場合には、前記読み取りを行った前記データを破棄して終了するステップと、

前記読み取りが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りを行って終了するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件を、前記読み取る方法で実行可能であるかを判定するステップと、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了するステップと、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りを行って終了するステップと、
を有する、セキュリティポリシーに基づいた文書の読み取り方法。

【請求項 2】 前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである、請求項 1 に記載のセキュリティポリシーに基づいた文書の読み取り方法。

【請求項 3】 前記実行可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである、請求項 1 あるいは 2 に記載のセキュリティポリシーに基づいた文書の読み取り方法。

【請求項 4】 前記表示可能なラベルは、少なくとも読み取りを指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む、請求項 3 に記載のセキュリティポリシーに基づいた文書の読み取り方法。

【請求項 5】 前記実行可能な要件は、少なくとも読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである、請求項 1 乃至 4 のうち何れか一項に記載のセキュリティポリシーに基づいた文書の読み取り方法。

【請求項 6】 請求項 1 乃至 5 のうち何れか一項に記載のセキュリティポリシーに基づいた文書の読み取り方法を、コンピュータに実行させる、セキュリティポリシーに基づいた文書の読み取りプログラム。

【請求項 7】 請求項 6 に記載のプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項 8】 請求項 6 に記載のプログラムを、コンピュータにネットワークを介して配信するプログラム伝送装置。

【請求項 9】 少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、
読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、
前記組み合わせで読み取りを実行する場合の要件と、
を備えるセキュリティポリシーに基づいた文書の読み取り装置であって、

前記読み取り装置は、
前記ユーザ属性を取得する手段と、
読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する手段と、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りが許可されているか否かを、前記セキュリティポリシーに基づいて判断する手段と

、
前記読み取りが許可されていないと判断した場合には、前記読み取りを行ったデータを破棄して終了する手段と、

前記読み取りが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りを行って終了する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件を、前記読み取り方法で実行可能であることを判定する手段と

、
実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了する手段と、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りを行って終了する手段と、
を有する、セキュリティポリシーに基づいた文書の読み取り装置。

【請求項 10】 前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである、請求項 9 に記載のセキュリティポリシーに基づいた文書の読み取り装置。

【請求項 11】 前記実行可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである、請求項 9 あるいは 10 に記載のセキュリティポリシーに基づいた文書の読み取り装置。

【請求項 12】 前記表示可能なラベルは、少なくとも読み取りを指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む、請求項

11 に記載のセキュリティポリシーに基づいた文書の読み取り装置。

【請求項 13】 前記実行可能な要件は、少なくとも読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである、請求項 9 乃至 12 のうち何れか一項に記載のセキュリティポリシーに基づいた文書の読み取り装置。

【請求項 14】 少なくともユーザカテゴリとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

ネットワーク配信を許可する前記文書属性と前記ユーザ属性との組み合わせと

、
前記組み合わせでネットワーク配信を実行する場合の要件と、
を備えるセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法であって、

前記文書を読み取り且つネットワーク配信を行う方法は、

前記ユーザ属性を取得するステップと、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得するステップと、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、前記文書の読み取りとネットワーク配信が許可されているか否かを、前記セキュリティポリシーに基づいて判断するステップと、

前記読み取りとネットワーク配信が許可されていないと判断した場合には、前記読み取りを行った前記データを破棄して終了するステップと、

前記文書の読み取りとネットワーク配信が許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りとネットワーク配信を行って終了するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には

、すべての前記要件が前記文書の読み取りとネットワーク配信を行う方法で実行可能であるかを判定するステップと、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了するステップと、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りとネットワーク配信を行って終了するステップと、
を有するセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項 15】 前記実行可能な要件が、前記読み取った文書データに電子透かしを埋め込むことである、請求項 14 に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項 16】 前記実行対応可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである、請求項 14 あるいは 15 に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項 17】 前記表示可能なラベルは、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む、請求項 15 に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項 18】 前記実行可能な要件は、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、ネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである、請求項 14 乃至 17 のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項 19】 前記実行可能な要件は、文書データを印刷不可能なデータに変換してネットワーク配信を行うことである、請求項 14 乃至 18 のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項 20】 前記印刷不可能なデータは、印刷禁止属性を持った PDF ファイルである、請求項 19 に記載のセキュリティポリシーに基づいて文書を読み

取り且つネットワーク配信を行う方法。

【請求項 2 1】 前記実行可能な要件が、信頼できるチャネルを利用してネットワーク配信を行うことである、請求項 1 4 乃至 2 0 のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法。

【請求項 2 2】 請求項 1 4 乃至 2 1 のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法をコンピュータに実行させる、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行うプログラム。

【請求項 2 3】 請求項 2 2 に記載のプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項 2 4】 請求項 2 2 に記載のプログラムをコンピュータにネットワーク配信するプログラム伝送装置。

【請求項 2 5】 少なくともユーザカテゴリとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

ネットワーク配信を許可する前記文書属性と前記ユーザ属性との組み合わせと

、
前記組み合わせでネットワーク配信を実行する場合の要件と、
を備えるセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置であって、

前記文書を読み取り且つネットワーク配信を行う装置は、

前記ユーザ属性を取得する手段と、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する手段と、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りとネットワーク配信が許可されているか否かを、前記セキュリティポリシーに基づ

いて判断する手段と、

前記文書を読み取り且つネットワーク配信を行うことが許可されていないと判断した場合には、前記読み取りを行ったデータを破棄して終了する手段と、

前記文書を読み取り且つネットワーク配信を行うことが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りとネットワーク配信を行って終了する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件が前記文書を読み取り且つネットワーク配信を行う方法で実行可能であるかを判定する手段と、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了する手段と、

すべての前記要件が実行可能である場合には、抽出された前記要件を満たして、前記文書を読み取り且つネットワーク配信を行って終了する手段と、
を有する、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項 26】 前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである、請求項 25 に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項 27】 前記実行可能な要件が、前記読み取った文書データに表示可能なラベルを埋め込むことである、請求項 25 あるいは 26 に記載のセキュリティポリシーに基づいた文書の読み取りとネットワーク配信を行う装置。

【請求項 28】 前記表示可能なラベルは、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む、請求項 27 に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項 29】 前記実行可能な要件は、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、ネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を

行うことである、請求項 25 乃至 28 のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項 30】 前記実行可能な要件が、文書データを印刷不可能なデータに変換してネットワーク配信を行うことである、請求項 25 乃至 29 のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項 31】 前記印刷不可能なデータは、印刷禁止属性を持った PDF ファイルである、請求項 30 に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項 32】 前記実行可能な要件が、信頼できるチャネルを利用してネットワーク配信を行うことである、請求項 25 乃至 31 のうち何れか一項に記載のセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置。

【請求項 33】 ドキュメントのセキュリティに関する取り扱いのルールを記述したドキュメントセキュリティポリシーに基づいて動作する入出力装置において、前記ドキュメントセキュリティポリシーを外部から設定することを特徴とする入出力装置。

【請求項 34】 前記ドキュメントセキュリティポリシーのルールには、少なくとも前記ドキュメントのセキュリティ属性とユーザのセキュリティ属性とオペレーションに対する、許可或は禁止、或は許可する場合の要件が記述されていることを特徴とする、請求項 33 記載の入出力装置。

【請求項 35】 設定された前記ドキュメントセキュリティポリシーの改ざん検知コードを検証することを特徴とする、請求項 33 或は 34 に記載の入出力装置。

【請求項 36】 設定された前記ドキュメントセキュリティポリシーのシリアル番号を記憶し、現在有効な前記ドキュメントセキュリティポリシーよりも新しいシリアル番号のドキュメントセキュリティポリシーが設定された場合にだけ、前記設定された前記ドキュメントセキュリティポリシーを有効なものとして利用することを特徴とする、請求項 33 乃至 35 に記載の入出力装置。

【請求項 37】 外部のサーバから前記ドキュメントセキュリティポリシーを受信することを特徴とする、請求項 33 乃至 36 に記載の入出力装置。

【請求項 38】 前記外部のサーバから前記ドキュメントセキュリティポリシーを受信する前に、前記外部のサーバの認証情報を受信し、受信した前記認証情報の検証を行うことを特徴とする、請求項 37 に記載の入出力装置。

【請求項 39】 前記外部のサーバから前記ドキュメントセキュリティポリシーを受信する前に、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする、請求項 37 或は 38 に記載の入出力装置。

【請求項 40】 前記外部のサーバへ前記ドキュメントセキュリティポリシーの前記送信要求を送信する前に、前記入出力装置自身の認証情報を送信することを特徴とする、請求項 39 に記載の入出力装置。

【請求項 41】 前記外部のサーバへポリシー送信要求を送信する前に、前記外部のサーバから前記ドキュメントセキュリティポリシーの送信通知を受信することを特徴とする、請求項 39 或は 40 に記載の入出力装置。

【請求項 42】 前記入出力装置の電源が投入されたときに、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする、請求項 39 或は 40 に記載の入出力装置。

【請求項 43】 前記入出力装置内部のタイマーに設定された時間に基づいて、前記外部サーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする、請求項 39 或は 40 に記載の入出力装置。

【請求項 44】 前記入出力装置を操作者が操作することにより、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする、請求項 39 或は 40 に記載の入出力装置。

【請求項 45】 取り外し可能な記憶媒体に記憶された前記ドキュメントセキュリティポリシーを読み取ることを特徴とする、請求項 33 乃至 36 に記載の入出力装置。

【請求項 46】 前記取り外し可能な記憶媒体から読み取った前記ドキュメントセキュリティポリシーを、内部記憶媒体に記憶し、前記外部サーバからの前記

ドキュメントセキュリティポリシー選択情報によって、前記記憶した前記ドキュメントセキュリティポリシーのうちから選択された前記ドキュメントセキュリティポリシーを利用することを特徴とする、請求項 45 に記載の入出力装置。

【請求項 47】 前記外部のサーバから前記ドキュメントセキュリティポリシー選択情報を受信する前に、前記外部のサーバの認証情報を受信し、受信した前記認証情報の検証を行うことを特徴とする、請求項 46 に記載の入出力装置。

【請求項 48】 前記入出力装置は、プリンタ、プリンタサーバ、スキャナ、スキャナサーバ、コピー、ファクシミリ、それらの複合機、或はドキュメント管理装置のいずれかであることを特徴とする、請求項 33 乃至 47 に記載の入出力装置。

【請求項 49】 ドキュメントのセキュリティに関する取り扱いのルールを記述したドキュメントセキュリティポリシーに基づいて動作するドキュメント処理ソフトウェアにおいて、前記前記ドキュメントセキュリティポリシーを外部から設定することを特徴とするドキュメント処理ソフトウェア。

【請求項 50】 ドキュメントセキュリティポリシーのルールには、少なくとも前記ドキュメントのセキュリティ属性とユーザのセキュリティ属性とオペレーションに対する、許可或は禁止、或は許可する場合の要件が記述されていることを特徴とする、請求項 49 に記載のドキュメント処理ソフトウェア。

【請求項 51】 設定された前記ドキュメントセキュリティポリシーの改ざん検知コードを検証することを特徴とする、請求項 49 或は 50 に記載のドキュメント処理ソフトウェア。

【請求項 52】 設定された前記ドキュメントセキュリティポリシーのシリアル番号を記憶し、現在有効な前記ドキュメントセキュリティポリシーよりも新しいシリアル番号のドキュメントセキュリティポリシーが設定された場合にだけ、前記設定された前記ドキュメントセキュリティポリシーを有効なものとして利用することを特徴とする、請求項 49 乃至 51 に記載のドキュメント処理ソフトウェア。

【請求項 53】 外部のサーバから前記ドキュメントセキュリティポリシーを受信することを特徴とする、請求項 49 乃至 52 に記載のドキュメント処理ソフトウェア。

トウェア。

【請求項 54】 前記外部のサーバから前記ドキュメントセキュリティポリシーを受信する前に、前記外部のサーバの認証情報を受信し、受信した前記認証情報の検証を行うことを特徴とする、請求項 53 に記載のドキュメント処理ソフトウェア。

【請求項 55】 前記外部のサーバから前記ドキュメントセキュリティポリシーを受信する前に、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする、請求項 53 或は 54 に記載のドキュメント処理ソフトウェア。

【請求項 56】 前記外部のサーバへ前記ドキュメントセキュリティポリシーの前記送信要求を送信する前に、前記ドキュメント処理ソフトウェア自身の認証情報を送信することを特徴とする、請求項 55 に記載のドキュメント処理ソフトウェア。

【請求項 57】 前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信する前に、前記外部のサーバから前記ドキュメントセキュリティポリシーの送信通知を受信することを特徴とする、請求項 55 或は 56 に記載のドキュメント処理ソフトウェア。

【請求項 58】 前記ドキュメント処理ソフトウェアが起動されたときに、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする、請求項 55 或は 56 に記載のドキュメント処理ソフトウェア。

【請求項 59】 前記ドキュメント処理ソフトウェアの内部のタイマーに設定された時間に基づいて、前記外部サーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする、請求項 55 或は 56 に記載のドキュメント処理ソフトウェア。

【請求項 60】 前記ドキュメント処理ソフトウェアを操作者が操作することにより、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする、請求項 55 或は 56 に記載のドキュメント処理ソフトウェア。

【請求項 6 1】 取り外し可能な記憶媒体に記憶された前記ドキュメントセキュリティポリシーを読み取ることを特徴とする、請求項 4 9 乃至 5 2 に記載のドキュメント処理ソフトウェア。

【請求項 6 2】 前記取り外し可能な記憶媒体から読み取った前記ドキュメントセキュリティポリシーを、内部記憶媒体に記憶し、前記外部サーバからの前記ドキュメントセキュリティポリシー選択情報によって、前記記憶した前記ドキュメントセキュリティポリシーのうちから選択された前記ドキュメントセキュリティポリシーを利用することを特徴とする、請求項 6 1 に記載のドキュメント処理ソフトウェア。

【請求項 6 3】 前記外部のサーバから前記ドキュメントセキュリティポリシー選択情報を受信する前に、前記外部のサーバの認証情報を受信し、受信した前記認証情報の検証を行うことを特徴とする、請求項 6 2 に記載のドキュメント処理ソフトウェア。

【請求項 6 4】 前記ソフトウェアは、プラグインであることを特徴とする、請求項 4 9 乃至 6 3 に記載のドキュメント処理ソフトウェア。

【請求項 6 5】 少なくともドキュメントのセキュリティに関する取り扱いのルールを記述したドキュメントセキュリティポリシーを管理するサーバと入出力装置からなるドキュメントシステムにおいて、前記入出力装置が前記サーバの管理している前記ドキュメントセキュリティポリシーに従って動作することを特徴とするドキュメントシステム。

【請求項 6 6】 前記ドキュメントセキュリティポリシーのルールには、少なくとも前記ドキュメントのセキュリティ属性とユーザのセキュリティ属性とオペレーションに対する、許可或は禁止或は許可する場合の要件が記述されていることを特徴とする、請求項 6 5 に記載のドキュメントシステム。

【請求項 6 7】 前記入出力装置が前記サーバに対して、少なくとも前記ドキュメントのセキュリティ属性と前記ユーザのセキュリティ属性と前記オペレーションの情報を送信し、前記サーバは前記入出力装置に対して、少なくとも許可あるいは禁止あるいは許可する場合の前記要件を送信することを特徴とする、請求項 6 5 或は 6 6 に記載のドキュメントシステム。

【請求項 68】 前記入出力装置が前記サーバに対して情報を送信する前に、前記入出力装置自身の認証情報を送信し、前記サーバは受信した前記認証情報の検証を行うことを特徴とする、請求項 67 に記載のドキュメントシステム。

【請求項 69】 前記サーバが前記入出力装置に情報を送信する前に、前記サーバ自身の認証情報を送信し、前記入出力装置は受信した前記認証情報の検証を行うことを特徴とする、請求項 67 或は 68 に記載のドキュメントシステム。

【請求項 70】 前記入出力装置は、プリンタ、プリンタサーバ、スキャナ、スキャナサーバ、コピー、ファクシミリ、それらの複合機、或はドキュメント管理装置のいずれかであることを特徴とする、請求項 65 乃至 69 に記載のドキュメントシステム。

【請求項 71】 少なくともドキュメントのセキュリティに関する取り扱いのルールを記述したドキュメントセキュリティポリシーを管理するサーバとドキュメント処理ソフトウェアからなるドキュメントシステムにおいて、前記ドキュメント処理ソフトウェアがサーバの管理している前記ドキュメントセキュリティポリシーに従って動作することを特徴とするドキュメントシステム。

【請求項 72】 前記ドキュメントセキュリティポリシーのルールには、少なくとも前記ドキュメントのセキュリティ属性とユーザのセキュリティ属性とオペレーションに対する、許可或は禁止、或は許可する場合の要件が記述されていることを特徴とする、請求項 71 に記載のドキュメントシステム。

【請求項 73】 前記ドキュメント処理ソフトウェアが、前記サーバに対して少なくとも前記ドキュメントのセキュリティ属性と前記ユーザのセキュリティ属性と前記オペレーションの情報を送信し、前記サーバは前記ドキュメント処理ソフトウェアに対して少なくとも許可あるいは禁止あるいは許可する場合の前記要件を送信することを特徴とする、請求項 71 或は 72 に記載のドキュメントシステム。

【請求項 74】 前記ドキュメント処理ソフトウェアが前記サーバに対して情報を送信する前に、前記ドキュメント処理ソフトウェア自身の認証情報を送信し、前記サーバは受信した前記認証情報の検証を行うことを特徴とする、請求項 73 に記載のドキュメントシステム。

【請求項 75】 前記サーバが前記ドキュメント処理ソフトウェアに情報を送信する前に、前記サーバ自身の認証情報を送信し、前記ドキュメント処理ソフトウェアは、受信した前記認証情報の検証を行うことを特徴とする、請求項 73 あるいは 74 記載のドキュメントシステム。

【請求項 76】 前記ドキュメント処理ソフトウェアは、プラグインの形態をとることを特徴とする、請求項 71 乃至 75 に記載のドキュメントシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報システムのセキュリティを確保するシステムに関し、特に、セキュリティポリシーに基づいた文書の読み取りとネットワーク配信を行う方法、装置、プログラム、記憶媒体、伝送装置及び、セキュリティポリシーを外部から設定する入出力装置に関連する。

【0002】

【従来の技術】

オフィスに代表されるような文書を扱うフィールドでは、その文書のセキュリティをコントロールしたいという要望が、常に存在する。例えば秘密の文書を複写する際には管理責任者の許可を得なければならない等、特に情報のコンテナであるドキュメントに対するポリシー、中でも機密保持に関するポリシーの制御が重要視される。一般に、情報システムのセキュリティ確保は機密性、完全性、可用性の確保に大別されるが、完全性や可用性はシステムの管理者が適切に運営、管理すれば実質上問題のないレベルまで確保できることが多い。これに対して、機密性の確保のためには、ユーザ組織に所属するメンバに、ポリシーを共有及び徹底させなければならないためであろうと推測される。

【0003】

現実には多くの企業では文書管理規定などを設け、セキュリティをコントロールしようとしている。しかし、実際のオフィスシステムにおけるセキュリティの確保については、文書についてのセキュリティではなく、オフィスシステムを構成するさまざまな機器に関して、個別にセキュリティ設定を行う必要がある。

【0004】

セキュリティポリシーに基づいてアクセス制御を行う方法に関する従来技術としては、種々のものが挙げられる（特許文献1から、特許文献14）。

【0005】

例えば、アクセス制御において、条件付のアクセス許可を評価することが記載されている（特許文献1）。

【0006】

また、例えば、情報セキュリティポリシーに従った企業情報システムのセキュリティ管理、監査の簡単化について記載されている（特許文献2）。

【0007】

しかし、特に、上述の特許文献1では、データファイルへのアクセス制御システムで、アクセス後のデータの処理、特に読み取りなどには言及されていない。

【0008】

また、上述の特許文献2では、セキュリティーポリシー、システム、制御手段から構成され、それぞれの組み合わせを登録してあるDB（データベース）から制御手段を抽出して、システムをポリシーに合うように制御する手段を有しているがしかし、その状態を監査する手段では、システムに対して登録された制御手段で制御するだけであり、実現の自由度が低い。

【0009】

また、特許文献7の操作者IDを入力させ、文書からIDを取り出し、複写を制御する方法では、複写を拒否する、又は、複写を許可してログを記録するという固定されたルールに基づく制御しか行えない。

【0010】

特許文献8の画像から機密文書であることを示すマークを取り出してチェックする方法では、得られた情報からどのような動作を行うかまでが決められているため、ルールの柔軟性に欠ける。

【0011】

特許文献9の印刷情報に含まれる出力制限データに基づいて出力先を制御する方法では、印刷情報にルールを含めなければならない。

【 0 0 1 2 】

特許文献 1 0 の画像を読み取ってパスワードとともに記憶し、出力の際にパスワードが一致したときに許可する方法では、判断する基準がパスワードだけであり、それによって制御される動作も許可、又は、不許可だけである。

【 0 0 1 3 】

特許文献 1 1 のネットワーク上の複数のMFPのうち、一つのMFPがユーザ管理を行ってネットワーク上のMFPすべての操作の許可、不許可を制御する方法では、制御される動作は許可、又は、不許可だけである。

【 0 0 1 4 】

特許文献 1 2 の複数の機器について利用の許可、操作の許可をユーザごとに判断する方法では、許可、不許可だけしか制御できないし、ユーザ情報に基づいた制御しかできない。というように、従来技術の問題点はルールが限定的で柔軟性がなく、またそのルールもあらかじめ決められたものだけであるという欠点がある。すなわち、従来の入出力装置は、「ユーザ」と「ドキュメント」のIDに対する、操作の「許可」、「禁止」だけを、「あらかじめ」決められているものばかりである。

【 0 0 1 5 】**【特許文献 1】**

特開 2 0 0 1 - 1 8 4 2 6 4 号公報

【特許文献 2】

特開 2 0 0 1 - 2 7 3 3 8 8 号公報

【特許文献 3】

特開 2 0 0 1 - 3 3 7 8 6 4 号公報

【特許文献 4】

特開平 0 9 - 2 9 3 0 3 6 号公報

【特許文献 5】

特開平 0 7 - 1 4 1 2 9 6 号公報

【特許文献 6】

特許第 0 2 7 3 5 9 6 6 号公報

【特許文献 7】

特許 3203103 号公報

【特許文献 8】

特開平 7-58950 号公報

【特許文献 9】

特開平 7-152520 号公報

【特許文献 10】

特開平 10-191072 号公報

【特許文献 11】

特開 2000-15898 号公報

【特許文献 12】

特開 2000-357064 号公報

【特許文献 13】

特開 2001-125759 号公報

【特許文献 14】

特開 2001-325249 号公報。

【0016】

【発明が解決しようとする課題】

このようなセキュリティの設定方法では、文書印刷のセキュリティ設定をする場合には、第 1 に、設定者が、さまざまな機器のセキュリティに関する知識を必要とする。そして、第 2 には、すべての機器に対してセキュリティが、一つ一つ設定される必要がある。第 3 には、システムの全体がどのようなセキュリティ状態になっているのかを容易に把握することが必要であるが、把握しにくい。そして、第 4 に、個々の機器にセキュリティ設定がされていても、実際に文書のセキュリティが守られていることが実感できない。このように、実際のオフィスシステムにおけるセキュリティの確保については、以上のような問題点がある。本発明は、上述の問題点を解決することを目的とする。

【0017】

特に本発明の目的は、文書に関するセキュリティポリシーに基づいて、紙文書

の読み取り、ネットワークへの配信を行う方法、その方法を実行するプログラム、そのプログラムを記憶した記憶媒体、文書の伝送装置および文書の読み取り装置を提供することである。

【0018】

更に、本発明は、文書の読み取り装置や印刷装置等又は、その複合機において、今まで決められたルールに従った動作しかできなかったという課題を解決するために、外部からセキュリティポリシーを設定できる入出力装置を提供することである。

【0019】

【課題を解決するための手段】

上記目的は、以下の本発明により解決される。

【0020】

請求項1に記載の発明では、セキュリティポリシーに基づいた文書の読み取り方法は、少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、
読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、
前記組み合わせで読み取りを実行する場合の要件と、
を備えるセキュリティポリシーに基づいた文書の読み取り方法であって、
前記読み取り方法は、
前記ユーザ属性を取得するステップと、
読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得するステップと、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りが許可されているか否かを、前記セキュリティポリシーに基づいて判断するステップと、

前記読み取りが許可されていないと判断した場合には、前記読み取りを行った前記データを破棄して終了するステップと、

前記読み取りが許可されていると判断した場合には、対応する要件を前記セキ

ユリティポリシーから抽出するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りを行って終了するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件を、前記読み取る方法で実行可能であることを判定するステップと、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了するステップと、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りを行って終了するステップと、
を有する。

【0021】

請求項2に記載の発明では、前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである。

【0022】

請求項3に記載の発明では、前記実行可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである。

【0023】

請求項4に記載の発明では、前記表示可能なラベルは、少なくとも読み取りを指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む。

【0024】

請求項5に記載の発明では、前記実行可能な要件は、少なくとも読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである。

【0025】

請求項6に記載の発明は、セキュリティポリシーに基づいた文書の読み取り方法を、コンピュータに実行させる、セキュリティポリシーに基づいた文書の読み取りプログラム。

【0026】

請求項7に記載の発明は、そのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【0027】

請求項8に記載の発明は、そのプログラムを、コンピュータにネットワークを介して配信するプログラム伝送装置である。

【0028】

請求項9に記載の発明では、セキュリティポリシーに基づいた文書の読み取り装置は、少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、
読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、
前記組み合わせで読み取りを実行する場合の要件と、
を備えるセキュリティポリシーに基づいた文書の読み取り装置であって、
前記読み取り装置は、
前記ユーザ属性を取得する手段と、
読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する手段と、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りが許可されているか否かを、前記セキュリティポリシーに基づいて判断する手段と

前記読み取りが許可されていないと判断した場合には、前記読み取りを行ったデータを破棄して終了する手段と、

前記読み取りが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りを行って終了する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件を、前記読み取り方法で実行可能であることを判定する手段と

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了する手段と、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前記文書の読み取りを行って終了する手段と、
を有する。

【0029】

請求項10に記載の発明では、前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである。

【0030】

請求項11に記載の発明では、前記実行可能な要件は、前記読み取った文書データに表示可能なラベルを埋め込むことである。

【0031】

請求項12に記載の発明では、前記表示可能なラベルは、少なくとも読み取りを指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む。

【0032】

請求項13に記載の発明では、前記実行可能な要件は、少なくとも読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである。

【0033】

請求項14に記載の発明では、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法は、少なくともユーザカテゴリーとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリーとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

ネットワーク配信を許可する前記文書属性と前記ユーザ属性との組み合わせと

前記組み合わせでネットワーク配信を実行する場合の要件と、
を備えるセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信
を行う方法であって、

前記文書を読み取り且つネットワーク配信を行う方法は、

前記ユーザ属性を取得するステップと、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する
ステップと、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、前記文書の
読み取りとネットワーク配信が許可されているか否かを、前記セキュリティポリ
シーに基づいて判断するステップと、

前記読み取りとネットワーク配信が許可されていないと判断した場合には、前
記読み取りを行った前記データを破棄して終了するステップと、

前記文書の読み取りとネットワーク配信が許可されていると判断した場合には
、対応する要件を前記セキュリティポリシーから抽出するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合に
は、前記文書の読み取りとネットワーク配信を行って終了するステップと、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には
、すべての前記要件が前記文書の読み取りとネットワーク配信を行う方法で実行
可能であるかを判定するステップと、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行った
データを破棄して終了するステップと、

すべての要件を実行可能である場合には、抽出された前記要件を満たして、前
記文書の読み取りとネットワーク配信を行って終了するステップと、
を有する。

【0034】

請求項15に記載の発明では、前記実行可能な要件が、前記読み取った文書デ
ータに電子透かしを埋め込むことである。

【0035】

請求項16に記載の発明では、前記実行対応可能な要件は、前記読み取った文

書データに表示可能なラベルを埋め込むことである。

【0036】

請求項 17 に記載の発明では、前記表示可能なラベルは、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む。

【0037】

請求項 18 に記載の発明では、前記実行可能な要件は、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、ネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである。

【0038】

請求項 19 に記載の発明では、前記実行可能な要件は、文書データを印刷不可能なデータに変換してネットワーク配信を行うことである。

【0039】

請求項 20 に記載の発明では、前記印刷不可能なデータは、印刷禁止属性を持った PDF ファイルである。

【0040】

請求項 21 に記載の発明では、前記実行可能な要件が、信頼できるチャネルを利用してネットワーク配信を行うことである。

【0041】

請求項 22 に記載の発明は、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う方法をコンピュータに実行させる、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行うプログラムである。

【0042】

請求項 23 に記載の発明は、そのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【0043】

請求項 24 に記載の発明は、そのプログラムをコンピュータにネットワーク配

信するプログラム伝送装置である。

【0044】

請求項 25 に記載の発明では、セキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置は、少なくともユーザカテゴリとセキュリティレベルを有するユーザ属性と、

少なくとも文書カテゴリとセキュリティレベルを有する文書属性と、

読み取りを許可する前記文書属性と前記ユーザ属性との組み合わせと、

前記組み合わせで読み取りを実行する場合の要件と、

ネットワーク配信を許可する前記文書属性と前記ユーザ属性との組み合わせと

前記組み合わせでネットワーク配信を実行する場合の要件と、
を備えるセキュリティポリシーに基づいて文書を読み取り且つネットワーク配信を行う装置であって、

前記文書を読み取り且つネットワーク配信を行う装置は、

前記ユーザ属性を取得する手段と、

読み取りを行った前記文書のデータから、前記文書の前記文書属性を取得する手段と、

取得した前記ユーザ属性と前記文書属性との組み合わせに対して、読み取りとネットワーク配信が許可されているか否かを、前記セキュリティポリシーに基づいて判断する手段と、

前記文書を読み取り且つネットワーク配信を行うことが許可されていないと判断した場合には、前記読み取りを行ったデータを破棄して終了する手段と、

前記文書を読み取り且つネットワーク配信を行うことが許可されていると判断した場合には、対応する要件を前記セキュリティポリシーから抽出する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在しない場合には、前記文書の読み取りとネットワーク配信を行って終了する手段と、

抽出されるべき前記要件が、前記セキュリティポリシー内に存在する場合には、すべての前記要件が前記文書を読み取り且つネットワーク配信を行う方法で実行可能であるかを判定する手段と、

実行可能でない前記要件が、存在する場合には、前記文書の読み取りを行ったデータを破棄して終了する手段と、

すべての前記要件が実行可能である場合には、抽出された前記要件を満たして、前記文書を読み取り且つネットワーク配信を行って終了する手段と、を有する。

【0045】

請求項26に記載の発明では、前記実行可能な要件は、前記読み取った文書データに電子透かしを埋め込むことである。

【0046】

請求項27に記載の発明では、前記実行可能な要件が、前記読み取った文書データに表示可能なラベルを埋め込むことである。

【0047】

請求項28に記載の発明では、前記表示可能なラベルは、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、読み取りを指示した時点のタイムスタンプを含む。

【0048】

請求項29に記載の発明では、前記実行可能な要件は、少なくとも読み取りとネットワーク配信を指示したユーザの認証データと、ネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録を行うことである。

【0049】

請求項30に記載の発明では、前記実行可能な要件が、文書データを印刷不可能なデータに変換してネットワーク配信を行うことである。

【0050】

請求項31に記載の発明では、前記印刷不可能なデータは、印刷禁止属性を持ったPDFファイルである。

【0051】

請求項32に記載の発明では、前記実行可能な要件が、信頼できるチャネルを利用してネットワーク配信を行うことである。

【0052】

以上本発明により、文書に関するセキュリティポリシーに基づいて、紙文書の読み取り、ネットワークへの配信を行う方法、その方法を実行するプログラム、そのプログラムを記憶した記憶媒体、文書の伝送装置および文書の印刷装置を提供することができる。

【0053】

請求項33に記載の発明は、ドキュメントのセキュリティに関する取り扱いのルールを記述したドキュメントセキュリティポリシーに基づいて動作する入出力装置において、前記ドキュメントセキュリティポリシーを外部から設定することを特徴とする入出力装置である。

【0054】

請求項34に記載の発明は、前記ドキュメントセキュリティポリシーのルールには、少なくとも前記ドキュメントのセキュリティ属性とユーザのセキュリティ属性とオペレーションに対する、許可或は禁止、或は許可する場合の要件が記述されていることを特徴とする入出力装置である。

【0055】

請求項35に記載の発明は、設定された前記ドキュメントセキュリティポリシーの改ざん検知コードを検証することを特徴とする入出力装置である。

【0056】

請求項36に記載の発明は、設定された前記ドキュメントセキュリティポリシーのシリアル番号を記憶し、現在有効な前記ドキュメントセキュリティポリシーよりも新しいシリアル番号のドキュメントセキュリティポリシーが設定された場合にだけ、前記設定された前記ドキュメントセキュリティポリシーを有効なものとして利用することを特徴とする入出力装置である。

【0057】

請求項37に記載の発明は、外部のサーバから前記ドキュメントセキュリティポリシーを受信することを特徴とする入出力装置である。

【0058】

請求項38に記載の発明は、前記外部のサーバから前記ドキュメントセキュリ

ティポリシーを受信する前に、前記外部のサーバの認証情報を受信し、受信した前記認証情報の検証を行うことを特徴とする入出力装置である。

【0059】

請求項39に記載の発明は、前記外部のサーバから前記ドキュメントセキュリティポリシーを受信する前に、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする入出力装置である。

【0060】

請求項40に記載の発明は、前記外部のサーバへ前記ドキュメントセキュリティポリシーの前記送信要求を送信する前に、前記入出力装置自身の認証情報を送信することを特徴とする入出力装置である。

【0061】

請求項41に記載の発明は、前記外部のサーバへポリシー送信要求を送信する前に、前記外部のサーバから前記ドキュメントセキュリティポリシーの送信通知を受信することを特徴とする入出力装置である。

【0062】

請求項42に記載の発明は、前記入出力装置の電源が投入されたときに、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする入出力装置である。

【0063】

請求項43に記載の発明は、前記入出力装置内部のタイマーに設定された時間に基づいて、前記外部サーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする入出力装置である。

【0064】

請求項44に記載の発明は、前記入出力装置を操作者が操作することにより、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とする入出力装置である。

【0065】

請求項45に記載の発明は、取り外し可能な記憶媒体に記憶された前記ドキュメントセキュリティポリシーを読み取ることを特徴とする入出力装置である。

【0066】

請求項46に記載の発明は、前記取り外し可能な記憶媒体から読み取った前記ドキュメントセキュリティポリシーを、内部記憶媒体に記憶し、前記外部サーバからの前記ドキュメントセキュリティポリシー選択情報によって、前記記憶した前記ドキュメントセキュリティポリシーのうちから選択された前記ドキュメントセキュリティポリシーを利用することを特徴とする入出力装置である。

【0067】

請求項47に記載の発明は、前記外部のサーバから前記ドキュメントセキュリティポリシー選択情報を受信する前に、前記外部のサーバの認証情報を受信し、受信した前記認証情報の検証を行うことを特徴とする入出力装置である。

【0068】

請求項48に記載の発明は、前記入出力装置は、プリンタ、プリンタサーバ、スキャナ、スキャナサーバ、コピー、ファクシミリ、それらの複合機、或はドキュメント管理装置のいずれかであることを特徴とする入出力装置である。

【0069】

請求項49に記載の発明は、ドキュメントのセキュリティに関する取り扱いのルールを記述したドキュメントセキュリティポリシーに基づいて動作するドキュメント処理ソフトウェアにおいて、前記前記ドキュメントセキュリティポリシーを外部から設定することを特徴とするドキュメント処理ソフトウェアである。

【0070】

請求項50に記載の発明は、ドキュメントセキュリティポリシーのルールには、少なくとも前記ドキュメントのセキュリティ属性とユーザのセキュリティ属性とオペレーションに対する、許可或は禁止、或は許可する場合の要件が記述されていることを特徴とするドキュメント処理ソフトウェアである。

【0071】

請求項51に記載の発明は、設定された前記ドキュメントセキュリティポリシーの改ざん検知コードを検証することを特徴とするドキュメント処理ソフトウェアである。

【0072】

請求項 52 に記載の発明は、設定された前記ドキュメントセキュリティポリシーのシリアル番号を記憶し、現在有効な前記ドキュメントセキュリティポリシーよりも新しいシリアル番号のドキュメントセキュリティポリシーが設定された場合にだけ、前記設定された前記ドキュメントセキュリティポリシーを有効なものとして利用することを特徴とするドキュメント処理ソフトウェアである。

【0073】

請求項 53 に記載の発明は、外部のサーバから前記ドキュメントセキュリティポリシーを受信することを特徴とするドキュメント処理ソフトウェアである。

【0074】

請求項 54 に記載の発明は、前記外部のサーバから前記ドキュメントセキュリティポリシーを受信する前に、前記外部のサーバの認証情報を受信し、受信した前記認証情報の検証を行うことを特徴とするドキュメント処理ソフトウェアである。

【0075】

請求項 55 に記載の発明は、前記外部のサーバから前記ドキュメントセキュリティポリシーを受信する前に、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とするドキュメント処理ソフトウェアである。

【0076】

請求項 56 に記載の発明は、前記外部のサーバへ前記ドキュメントセキュリティポリシーの前記送信要求を送信する前に、前記ドキュメント処理ソフトウェア自身の認証情報を送信することを特徴とするドキュメント処理ソフトウェアである。

【0077】

請求項 57 に記載の発明は、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信する前に、前記外部のサーバから前記ドキュメントセキュリティポリシーの送信通知を受信することを特徴とするドキュメント処理ソフトウェアである。

【0078】

請求項 58 に記載の発明は、前記ドキュメント処理ソフトウェアが起動されたときに、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とするドキュメント処理ソフトウェアである。

【0079】

請求項 59 に記載の発明は、前記ドキュメント処理ソフトウェアの内部のタイマーに設定された時間に基づいて、前記外部サーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とするドキュメント処理ソフトウェアである。

【0080】

請求項 60 に記載の発明は、前記ドキュメント処理ソフトウェアを操作者が操作することにより、前記外部のサーバへ前記ドキュメントセキュリティポリシーの送信要求を送信することを特徴とするドキュメント処理ソフトウェアである。

【0081】

請求項 61 に記載の発明は、取り外し可能な記憶媒体に記憶された前記ドキュメントセキュリティポリシーを読み取ることを特徴とするドキュメント処理ソフトウェアである。

【0082】

請求項 62 に記載の発明は、前記取り外し可能な記憶媒体から読み取った前記ドキュメントセキュリティポリシーを、内部記憶媒体に記憶し、前記外部サーバからの前記ドキュメントセキュリティポリシー選択情報によって、前記記憶した前記ドキュメントセキュリティポリシーのうちから選択された前記ドキュメントセキュリティポリシーを利用することを特徴とするドキュメント処理ソフトウェアである。

【0083】

請求項 63 に記載の発明は、前記外部のサーバから前記ドキュメントセキュリティポリシー選択情報を受信する前に、前記外部のサーバの認証情報を受信し、受信した前記認証情報の検証を行うことを特徴とするドキュメント処理ソフトウェアである。

【0084】

請求項 64 に記載の発明は、前記ソフトウェアは、プラグインであることを特徴とするドキュメント処理ソフトウェアである。

【0085】

請求項 65 に記載の発明は、少なくともドキュメントのセキュリティに関する取り扱いのルールを記述したドキュメントセキュリティポリシーを管理するサーバと入出力装置からなるドキュメントシステムにおいて、前記入出力装置が前記サーバの管理している前記ドキュメントセキュリティポリシーに従って動作することを特徴とするドキュメントシステムである。

【0086】

請求項 66 に記載の発明は、前記ドキュメントセキュリティポリシーのルールには、少なくとも前記ドキュメントのセキュリティ属性とユーザのセキュリティ属性とオペレーションに対する、許可或は禁止或は許可する場合の要件が記述されていることを特徴とするドキュメントシステムである。

【0087】

請求項 67 に記載の発明は、前記入出力装置が前記サーバに対して、少なくとも前記ドキュメントのセキュリティ属性と前記ユーザのセキュリティ属性と前記オペレーションの情報を送信し、前記サーバは前記入出力装置に対して、少なくとも許可あるいは禁止あるいは許可する場合の前記要件を送信することを特徴とするドキュメントシステムである。

【0088】

請求項 68 に記載の発明は、前記入出力装置が前記サーバに対して情報を送信する前に、前記入出力装置自身の認証情報を送信し、前記サーバは受信した前記認証情報の検証を行うことを特徴とするドキュメントシステムである。

【0089】

請求項 69 に記載の発明は、前記サーバが前記入出力装置に情報を送信する前に、前記サーバ自身の認証情報を送信し、前記入出力装置は受信した前記認証情報の検証を行うことを特徴とするドキュメントシステムである。

【0090】

請求項 70 に記載の発明は、前記入出力装置は、プリンタ、プリンタサーバ、

スキャナ、スキャナサーバ、コピー、ファクシミリ、それらの複合機、或はドキュメント管理装置のいずれかであることを特徴とするドキュメントシステムである。

【0091】

請求項71に記載の発明は、少なくともドキュメントのセキュリティに関する取り扱いのルールを記述したドキュメントセキュリティポリシーを管理するサーバとドキュメント処理ソフトウェアからなるドキュメントシステムにおいて、前記ドキュメント処理ソフトウェアがサーバの管理している前記ドキュメントセキュリティポリシーに従って動作することを特徴とするドキュメントシステムである。

【0092】

請求項72に記載の発明は、前記ドキュメントセキュリティポリシーのルールには、少なくとも前記ドキュメントのセキュリティ属性とユーザのセキュリティ属性とオペレーションに対する、許可或は禁止、或は許可する場合の要件が記述されていることを特徴とするドキュメントシステムである。

【0093】

請求項73に記載の発明は、前記ドキュメント処理ソフトウェアが、前記サーバに対して少なくとも前記ドキュメントのセキュリティ属性と前記ユーザのセキュリティ属性と前記オペレーションの情報を送信し、前記サーバは前記ドキュメント処理ソフトウェアに対して少なくとも許可あるいは禁止あるいは許可する場合の前記要件を送信することを特徴とするドキュメントシステムである。

【0094】

請求項74に記載の発明は、前記ドキュメント処理ソフトウェアが前記サーバに対して情報を送信する前に、前記ドキュメント処理ソフトウェア自身の認証情報を送信し、前記サーバは受信した前記認証情報の検証を行うことを特徴とするドキュメントシステムである。

【0095】

請求項75に記載の発明は、前記サーバが前記ドキュメント処理ソフトウェアに情報を送信する前に、前記サーバ自身の認証情報を送信し、前記ドキュメント

処理ソフトウェアは、受信した前記認証情報の検証を行うことを特徴とするドキュメントシステムである。

【0096】

請求項76に記載の発明は、前記ドキュメント処理ソフトウェアは、プラグインの形態をとることを特徴とするドキュメントシステムである。

【0097】

以上のように、本発明により、読取装置、印刷装置又は、複写装置又は、これらの組合せの複合機等に、セキュリティポリシーを外部より設定することも可能である。

【0098】

【発明の実施の形態】

本発明の実施例を、以下に詳細に説明する。

【0099】

先ず最初に、本発明の第1の実施例のセキュリティポリシーについて説明する。

【0100】

本実施例では、異なるタイプのシステムでドキュメントに対するセキュリティポリシーを共有するために、以下のような仕組みを使用して、セキュリティポリシーを記述する。ここでは、記述したセキュリティポリシーのことをドキュメントセキュリティポリシー（DSP）と呼ぶ。

【0101】

図1は、セキュリティポリシーの例を示す。ユーザの属する組織は、例えば、機密文書、丸秘文書、社外秘文書のような、文書の機密レベルごとに、ドキュメントに対して、例えば、図1のようなセキュリティポリシーを掲げることが想定される。

【0102】

このようなポリシーをDSPとして記述できるようにするために、以下のような方法を使用する。

【0103】

まず最初に、ドキュメントを機密レベル（極秘、丸秘、社外秘など）と、カテゴリ（人事文書、技術文書など）に応じて分類する。この、機密レベルとカテゴリの組みを、ドキュメントのセキュリティラベルと呼ぶ。このセキュリティラベルは、実際には、個々のドキュメントに属性情報として付与される。

【0104】

上記のような、分類の仕方の一例を、図16に示す。図16は、document_label_terminology.xmlファイルのリストの例を示す。

【0105】

DSPには、ドキュメントの機密レベル及びカテゴリに応じて、ドキュメントに対して許可される操作（オペレーション）を規定し、そして、その操作を許可する際に実行されるべき要件（管理責任者の許可を得る、ラベルを印刷する、など）を指定できるようにする必要がある。そのような、ドキュメントの機密レベル及びカテゴリを記述するのが、図2のdocument_label_terminology.xmlファイルである。図2においては、社内一般文書、人事関連文書及び技術関連文書のような、文書カテゴリの種類が設けられている。また、社外秘、秘、極秘のような、文書のセキュリティレベルの種類が設けられている。

【0106】

図3から図13は、policy_terminology.xmlファイルのリストの例を示す図（1）から（11）を示す。図3から図13により、1つのpolicy_terminology.xmlファイルを構成する。

【0107】

図3から図13のpolicy_terminology.xmlファイルのリストの例に示すように、policy_terminology.xmlファイルは、システムタイプの分類を記述する。そして、そのシステムタイプごとに、オペレーションを列挙する。そして、そのオペレーションごとに、オペレーションの実行の際にサポート可能な要件を列挙しておく。例えば、図3においては、システムタイプの種類として、複写機、プリンタ、ファクシミリ、スキャナ等が記述される。そして、例えば、図4に示されたように、複写機に関わるオペレーションとして、紙から紙への複写等が記述される。更に、例えば、図6に示すように、複写に関わる要件として、明示な許可、

監査証拠の記録等が記述される。

【0 1 0 8】

図 1 4 から図 2 3 は、policy.xml のファイルのリストの例を示す図 (1) から (1 0) を示す。図 1 4 から図 2 3 により、1 つの policy.xml のファイルを構成する。

【0 1 0 9】

上述の図 2 に示す定義ファイル document_label_terminology.xml と、図 3 から図 1 3 の policy_terminology.xml ファイルをもとにして、ユーザ組織のセキュリティに対するポリシーを DSP として例えば図 1 4 から図 2 3 に示す policy.xml ファイルのリストのように記述する。

【0 1 1 0】

次に、図 1 4 から図 2 3 の policy.xml ファイルのリストに示された、DSP の構造を、図 2 4 から 2 6 を参照して、以下に、詳しく説明する。

【0 1 1 1】

図 2 4 は、DSP の識別情報の例を示す図である。図 1 4 に示された policy.xml のファイルのリストの例に記載されているように、DSP の先頭には、その DSP の識別情報を記述する。DSP の識別情報は、図 2 4 に示されたように、<about_this_policy> と、</about_this_policy> で囲まれた範囲に記載される。

【0 1 1 2】

DSP の識別情報には、先ず最初に、この DSP を他の DSP と区別するために必要な、シリアル番号を、
<serial_number>RDSP0100-00000000000012-2023</serial_number> に示すように、記述する。

【0 1 1 3】

次に、適用した定義ファイルである policy_terminology.xml ファイルのシリアル番号を、
<terminology_applied>RDST0100-00000000000001-9487</terminology_applied> のように記述する。定義ファイルについても更新される可能性があるため、この DSP がどの定義ファイルに基づいて記述されているのかを明確にするために記録

しておく。

【0114】

次に、このDSPのタイトル、バージョン番号、作成日時、作成者、説明といった一般的な書誌情報を記録する。

【0115】

そして、DSPの識別情報は、`</about_this_policy>`により終了する。

【0116】

次に、上述のDSPの識別情報に続いて、ポリシーの内容を`<policy>`と`</policy>`で囲まれた範囲に記述する。図25は、ポリシーの内容を示す一実施例を示す。

【0117】

ポリシーの内容は、以下に説明するように、階層構造を用いて記録する。

【0118】

ポリシー`<policy>`は、複数のアクセス制御ルール`<acc_rule>`で構成される。一つのアクセス制御ルール`<acc_rule>`は、対象とするドキュメントのカテゴリ`<doc_category>`とレベル`<doc_security_level>`を一意に指定し、さらにアクセス制御リスト`<acl>`を一つ含むように構成される。

【0119】

アクセス制御リスト`<acl>`は、複数のアクセス制御エレメント`<ace>`で構成される。

【0120】

各アクセス制御エレメント`<ace>`は、対象とするユーザのカテゴリ`<user_category>`とレベル`<user_security_level>`を一意に指定し、さらに複数のオペレーション`<operation>`で構成される。

【0121】

各`<operation>`は、一つのオペレーション名`<name>`と、一つの禁止`<denied/>`、または一つの許可`<allowed/>`、または複数の`<requirement>`で構成される。

【0122】

ドキュメントのカテゴリ`<doc_category>`やユーザのカテゴリ`<user_category_level>`に記述している”ANY”は、どのカテゴリ、及び、レベルにも適用されるこ

とを示している。また、ユーザのカテゴリ<user_category>の” DOC-CATEGORY” は、ユーザのカテゴリがドキュメントのカテゴリと同じときに適用されることを示している。

【0123】

この実施例では、禁止するオペレーションには<denied/>を指定するようにしているが、DSPに記載されていなければアクセスは許可されていないことを表している、というように構成してもよい。

【0124】

このように、DSPを記述することにより、ドキュメントのタイプ（カテゴリ、レベル）に応じて、どのようなユーザタイプ（カテゴリ、レベル）が、ドキュメントに対してどのようなオペレーションが可能なのかを記述できる。そして更に、そのドキュメントについて、ユーザが、オペレーションが可能な場合には、どのような要件を満たさなければならないのかを明確に記述することができる。

【0125】

そして、DSPを、上記のようにプラットフォームに依存しないXMLで記述することにより、異なるタイプのシステム間で、このDSPを共通に利用することができる。特に、セキュリティポリシーを適用したい対象は、電子的なドキュメントに限らず、紙のドキュメントに対しても適用できなければならないため、図3から図13のpolicy_terminology.xmlファイルや図15から図23のpolicy.xmlファイルに記述しているように、紙ドキュメントに関するオペレーション（hardcopy，scanなど）も規定できる。

【0126】

本実施例の、図25に示す要件の中に、以下の<requirement>explicit_authorization</requirement>

が存在する。これは、「ドキュメントの管理責任者により明示的な許可が得られた場合には、そのオペレーションを許可する」という要件である。すべて、このDSPに従ってオペレーションがコントロールされるようになると、自由度が無くなる恐れが生じる。しかし、この明示的な許可という要件を指定できるようにすることにより、柔軟なオペレーションコントロールが可能となる。

【0127】

また、本実施例の特徴として、その「明示的な許可」という要件を指定可能にすることによって、明示的な許可が得られれば実行してもよいオペレーションと、明示的な許可が得られたとしても禁止しなければならないオペレーションとを区別することができるということである。

【0128】

従って、DSPに記載しないか又は、<denied/>で指定されたオペレーションは明示的な許可が得られたとしても禁止しなければならないオペレーションである。これにより、ポリシーを記述している側の意図を、的確に規定できるようになり、誤って許可を与えてしまつてオペレーションが実行されてしまうというような事態をあらかじめ防ぐように規定することができる。

【0129】

次に本発明のDSPの別の記述形式の実施例を、図26に示す。無条件で許可するオペレーションや、禁止するオペレーションが多くなつた場合には、オペレーションごとに<operation><allowed/></operation>というような入れ子構造を記述するのは効率が悪いので、無条件で許可するオペレーションを列挙する、<allowed_operations>と、許可しないオペレーションを列挙する、<denied_operations>を使用するようにしても良い。

【0130】

図27は、上述のDSPを蓄積し且つ配布する種々の媒体を示す。

【0131】

以上で説明したように、図27に示されたDSP50は、XML (E x t e n s i b l e M a r k u p L a n g u a g e) で記述されている。そして、電子的なファイルとして記録しておくことができる。また、その電子的なファイルを格納した、例えば、ハードディスク51、光磁気ディスク52、フレキシブルディスク53、又は、CD-ROM、CD-R、CD-RW、DVD、DVD-R、DVD-RAM、DVD-RW、DVD+RW、DVD+Rのような光ディスク54のような記憶媒体を作成することができる。また、その電子的なDSPをコンピュータ55を使用して、ネットワーク56を介してで伝送することができる。

【0132】

このDSPは、特定のシステム向けのセキュリティポリシーの記述ではなく、異なる複数のシステムで共通に利用できるセキュリティポリシーの記述である。従って、このセキュリティポリシー記述を記憶した記憶媒体を作成し、そして配布したり又は、ネットワーク経由して伝送したりすることにより、複数のシステムで共通に利用しやすくなる。

【0133】

次に、本発明の第2の実施例について説明する。図28は、本発明のセキュリティポリシーに基づいて動作する入出力装置の一例としての読取装置の実施例について説明する。しかし本発明は、他の入出力装置である、印刷装置や複写装置にも適用できる。

【0134】

本発明の第2の実施例を、図28及び図29を参照して以下に詳細に説明する。

【0135】

図28は、本発明の実施例の文書読み取り装置の構成を示す図である。また、図29は、XML (Extensible Markup Language) により記述した、本発明の実施例のセキュリティポリシーを示す。

【0136】

図28に示す本発明の実施例の文書読み取り装置100は、主に、オペレーションパネル101、データベース102、ユーザ属性取得手段103、文書属性取得手段104、セキュリティポリシー105、読み取り手段106、読み取りデータ107及びネットワークポート108より構成される。

【0137】

オペレーションパネル101には、読み取り支持110が入力される。

【0138】

図28においては、読み取り装置は、専用のハードウェアにより構成するように記載されているが、汎用のコンピュータとそのコンピュータ上で実行されるプログラムにより構成されても良い。また、以下に説明する本発明の実施例をコン

コンピュータ上で実行するプログラムは、コンピュータにより読み出し可能な記録媒体に記録され、その実行前に、コンピュータにより読みこまれる。また、このようなプログラムは、コンピュータネットワークを介して配信されることも可能である。

【0139】

図29は、XMLにより記述した、セキュリティポリシーであり、つぎのようにルール1からルール3を示す。

【0140】

ルール1は、図29の第4行目の<acc_rule>から、第10行目の<user_security_level>ANY</user_security_level>までの部分及び、第11行目<operation>から、第14行目</operation>までの部分により記述される。

【0141】

第5行目の <doc_category>ANY</doc_category>は、文書カテゴリーにかかわらずルール1が適用されることを示す。

【0142】

第6行目の<doc_security_level>basic</doc_security_level>は、文書のセキュリティレベルがbasicのときを示す。

【0143】

第9行目の<user_category>ANY</user_category>は、ユーザのカテゴリーにかかわらないことを示す。

【0144】

第10行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわらないことを示す。

【0145】

更に第12行目と第13行目の<name>scan</name>及び<allowed/>は、読み取りは要件なく許可されることを示す。

【0146】

従って、ルール1では、第5行目、第6行目、第9行目、第10行目、第12行目及び第13行目により、文書カテゴリーにかかわりなく、文書のセキュリティ

イレベルが” basic” の場合には、ユーザのカテゴリにかかわらず、且つ、ユーザのセキュリティレベルにかかわらず、読み取りは要件なく許可される。

【0 1 4 7】

次に、ルール 2 は、図 2 9 の第 4 行目の<acc_rule>から、第 1 0 行目の<user_security_level>ANY</user_security_level>までの部分及び、第 1 5 行目<operation>から、第 2 0 行目</operation>までの部分により記述される。

【0 1 4 8】

第 5 行目の <doc_category>ANY</doc_category>は、文書カテゴリにかかわらずルール 2 が適用されることを示している。

【0 1 4 9】

第 6 行目の<doc_security_level>basic</doc_security_level>は、文書のセキュリティレベルがbasicのときを示す。

【0 1 5 0】

第 9 行目の<user_category>ANY</user_category>は、ユーザのカテゴリにかかわらずを示す。

【0 1 5 1】

第 1 0 行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわらずを示す。

【0 1 5 2】

更に、第 1 6 行目から第 1 9 行目の

<name>net_delivery</name>

<requirement>audit</requirement>

<requirement>print_restriction</requirement>

<requirement>trusted_channel</requirement>

は、ネットワーク配信は、「ログを記録すること」と、「プリント制限をかけること」、「信頼できるチャネルを使用すること」の要件を満たすときに許可されることを示す。

【0 1 5 3】

従って、ルール 2 では、第 5 行目、第 6 行目、第 9 行目、第 1 0 行目、第 1 6

行目から第19行目により、文書カテゴリーにかかわらず、文書のセキュリティレベルが” basic” の場合には、ユーザのカテゴリーにかかわらず、且つ、ユーザのセキュリティレベルにかかわらず、ネットワーク配信は、ログを記録することと、プリント制限をかけること、信頼できるチャネルを使用することの要件を満たすときに許可されることを示している。

【0154】

そして、ルール3は、図29の第24行目の<acc_rule>から、第30行目の<user_security_level>ANY</user_security_level>までの部分及び、第31行目<operation>から、第35行目</operation>までの部分により記述される。

【0155】

第25行目の<doc_category>ANY</doc_category>は、文書カテゴリーにかかわりないことを示す。

【0156】

第26行目の<doc_security_level>high</doc_security_level>は、文書のセキュリティレベルがhighの場合を示す。

【0157】

第29行目の<user_category>DOC-CATEGORY</user_category>は、ユーザのカテゴリーが文書のカテゴリーと同じであることを示す。

【0158】

第30行目の<user_security_level>ANY</user_security_level>は、ユーザのセキュリティレベルにかかわりないことを示す。

【0159】

第32行目から第34行目の、
<name>scan</name>
<requirement>audit</requirement>
<requirement>embed_trace_info</requirement>
は、読み取りは、「ログを記録すること」及び、「追跡可能な情報を埋め込むこと」の要件を満たすときに許可される。

【0160】

従って、ルール 3 では、第 25 行目、第 26 行目、第 29 行目、第 30 行目、第 31 行目から第 34 行目により、文書カテゴリーにかかわらず、文書のセキュリティレベルが” high” の場合には、ユーザのカテゴリーが文書のカテゴリーと同じであり、且つ、ユーザのセキュリティレベルにかかわらず、読み取りは、ログを記録することと、追跡可能な情報を埋め込むことの要件を満たすときに許可されることを示している。

【0161】

ここで、「追跡可能な情報を埋め込むこと」には、例えば、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加などを含んでも良い。また、表示可能なラベルは、読み取りを指示したユーザの認証データと読み取りを指示した時点のタイムスタンプを含んでもよい。さらに、「ログを記録すること」には、読み取りを指示したユーザの認証データと、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録するようにしてもよい。また、「ログを記録すること」には、ネットワーク配信を指示したユーザの認証データとネットワーク配信先の情報と、読み取り対象の文書データと、読み取りを指示した時点のタイムスタンプをログに記録するようにしてもよい。

【0162】

次に、図 29 に示したセキュリティポリシーを使用して、図 28 に示した本発明の実施例の文書読み取り装置が文書を読み取り又は、読み取った文書をネットワークに配信する場合の実施例について説明する、

先ず最初に、文書読み取り装置が文書を読み取る場合の実施例について説明する。

【0163】

先ず最初に、ステップ A1 で、ユーザが、読み取り装置 100 に紙文書を設置し、オペレーションパネル 101 から、紙文書の読み取り指示 110 を入力する。

【0164】

次に、ステップ A2 で、読み取り手段 106 が、紙文書の読み取りを行う。

【0165】

次に、ステップA3で、文書属性取得手段104は、読み取った文書データのバーコードや電子透かしなどの画像情報から、文書IDを抽出し、データベース102に登録されている文書IDに対応するカテゴリ、セキュリティレベルを取得し、読み取り手段106に通知する。

【0166】

次に、ステップA4で、読み取り手段106は、上記の文書属性取得手段104が通知した文書属性に従って、セキュリティポリシー105の中の対応するエントリを検索して、要件を抽出する。

【0167】

上述の図29に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが”basic”の文書を読み取りしようとしている場合には、抽出すべき要件はない。

【0168】

また、上述の図29に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが”high”の文書を読み取りしようとしている場合には、前述のように、「ログを記録すること」及び「追跡可能な情報を埋め込むこと」が、読み取りの要件となる。「ログを記録すること」及び「追跡可能な情報を埋め込むこと」の内容に関しては、上述と同様である。

【0169】

次に、ステップA5-1で、上述のステップ4のセキュリティレベルが”basic”のときの場合のように、抽出すべき要件がない場合には、読み取り手段は文書の読み取りを行って、ユーザは文書データを取得して終了する。

【0170】

一方、ステップA5-2では、上述のステップ4のセキュリティレベルが”high”のときの場合のように、抽出すべき要件がある場合には、読み取り手段はその要件をすべて満たすことができるかを判定する。

【0171】

ステップA5-2の場合には、次に以下のステップ6-1と6-2が実行される。

【0172】

ステップA6-1では、すべての要件を満たすことができない場合は、ユーザに通知をして、読み取りデータを破棄して終了する。

【0173】

次に、ステップA6-2では、すべての要件を満たすことができる場合は、その要件を満たした読み取りを行って、ユーザは文書データを取得して終了する。この場合には、ステップA6-2では、以下のステップ、A7-1からA7-6が実行される。

【0174】

ステップA7-1では、ユーザ属性取得手段103は、オペレーションパネル101から読み取り指示110を出したユーザに、ユーザIDの入力要求を出す。

【0175】

次に、ステップA7-2では、ユーザは、オペレーションパネル101からユーザIDを入力する。

【0176】

次に、ステップA7-3では、ユーザ属性取得手段103は、ユーザIDからデータベース102に登録されている入力されたユーザIDに対応するカテゴリー、セキュリティレベルを取得し、読み取り手段106に通知する。

【0177】

次に、ステップA7-4では、ログを記録する。

【0178】

そして、ステップA7-5では、読み取った文書データに追跡可能な情報の埋め込み(例えば、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加など)を行う。表示可能なラベルは、読み取りを指示したユーザの認証データと読み取りを指示した時点のタイムスタンプを含んでもよい。

【0179】

最後に、ステップA7-6で、ユーザは文書データを、読み取りデータ107内に取得して終了する。

【0180】

以上のように、図29に示したセキュリティポリシーを使用して、図28に示した本発明の実施例の文書読み取り装置が文書を読み取ることができる。

【0181】

次に、文書読み取り装置が文書を読み取り且つ読み取った文書をネットワークに配信する場合の実施例について説明する。

【0182】

先ず最初に、ステップB1で、ユーザが、読み取り装置106に紙文書をセットし、オペレーションパネル106から、読み取りデータの配信先の指定及び紙文書の読み取り指示110を出す。

【0183】

次に、ステップB2で、読み取り手段106が、紙文書の読み取りを行う。

【0184】

次に、ステップB3で、文書属性取得手段104は、読み取った文書データのバーコードや電子透かしなどの画像情報から文書IDを抽出し、データベース102に登録されている文書IDに対応するカテゴリー、セキュリティレベルを取得し、読み取り手段106に通知する。

【0185】

次に、ステップB4では、読み取り手段106は、上記の文書属性取得手段104が通知した文書属性に従って、セキュリティポリシー105の中の対応するエントリを検索し、要件を抽出する。

【0186】

上述の図29に示すセキュリティポリシーに基づいて、例えば、セキュリティレベルが”basic”の文書を読み取り、ネットワーク配信しようとしている場合には、読み取りに関する要件はない。しかし、上述のように、ネットワークに配信する時には、「ログを記録すること」と「プリント制限をかけること」と「信頼できるチャネルを使用すること」が要件となる。

【0187】

また、上述の図29に示すセキュリティポリシーに基づいて、例えば、セキユ

リティレベルが” high” の文書を読み取りしようとしている場合には、読み取りに関する要件として、「ログを記録すること」と「追跡可能な情報を埋め込むこと(例えば、上述のような、電子すかしの埋め込み、表示可能なラベルの埋め込み、文書属性情報の追加など)」が要件となる。しかし、ネットワークに配信することを許可するルールがないため、許可されない。

【0188】

次に、例えば、文書をネットワークへ配信する際の要件が、セキュリティポリシー 105 内に存在しない場合には、ステップ B 5-1 では、読み取り手段 106 は文書をネットワークポート 108 を介してネットワークへ配信して、処理を終了する。

【0189】

一方、例えば、文書をネットワークへ配信する際の要件が、セキュリティポリシー 105 内に存在する場合には、ステップ 5-2 で、読み取り手段 106 が、その要件をすべて満たすことができるかを判定する。

【0190】

ステップ B 5-2 の場合には次に、ステップ B 5-3 で、ネットワークに配信することを許可するルールがない場合には、読み取り手段 106 が、ユーザに、「ネットワークに配信することを許可するルールがない」ことを通知をして、読み取りデータを破棄して終了する。例えば、これは、上述のステップ B 4 の、セキュリティレベルが” high” の場合である。

【0191】

次に、ステップ B 6-1 では、すべての要件を満たすことができない場合は、ユーザに通知をして、読み取りデータを破棄して終了する。

【0192】

次に、ステップ B 6-2 では、例えば、上述のセキュリティレベルが” basic” の場合のように、すべての要件を満たすことができる場合は、その要件を満たした読み取り及び、文書をネットワークに配信して終了する。この場合には、ステップ B 6-2 では、以下のステップ、B 7-1 から B 7-6 が実行される。

【0193】

ステップB7-1では、ユーザ属性取得手段106は、オペレーションパネル101から、読み取り指示110を出したユーザに、ユーザIDの入力要求を出す。

【0194】

次に、ステップB7-2では、ユーザは、オペレーションパネル101からユーザIDを入力する。

【0195】

次に、ステップB7-3では、ユーザ属性取得手段103は、ユーザIDからデータベース102に登録されている入力されたユーザIDに対応するカテゴリー、セキュリティレベルを取得し、読み取り手段106に通知する。

【0196】

次に、ステップB7-4では、ログを記録する。

【0197】

そして、ステップB7-5では、読み取った文書データを、印刷不可能なデータ(たとえばADOBE(登録商標)の印刷禁止属性を持ったPDFなど)に変換する。

【0198】

最後にステップB7-6では、信頼できる通信経路(たとえばIPsecやVPNなど)を通じて、文書を、ネットワークポート108を介してネットワークへ配信し、終了する。

【0199】

以上のように、図29に示したセキュリティポリシーを使用して、図28に示した本発明の実施例の文書読み取り装置が、文書を読み取り且つ読み取った文書をネットワークに配信することができる。

【0200】

次に、本発明のセキュリティポリシーを、入出力装置の一例としての、上述の読取装置、印刷装置又は、複写装置又は、これらの組合せの複合機に設定する実施例について、以下に説明する。

【0201】

次に、本発明の第3の実施例について説明する。図30は、本発明の第3の実

施例を示す図である。図30は、ネットワークポートを通じて外部からセキュリティポリシーを受信し、内部のポリシーDB（データターベース）に保存する複合機3000の実施例である。図30に示す複合機3000は、上述した、読取装置、印刷装置又は、複写装置又は、これらの組合せの複合機を構成する。複合機3000は、複合機エンジン3001、CPU（中央処理装置）3002、ポリシーDB3003、アプリケーション3004及びネットワーク3006に接続されたネットワークポート3005より構成される。

【0202】

CPU3002は、アプリケーション3004の指示に従って、ネットワークポート3005を通じて外部からポリシーを受信し、内部のポリシーDB3003に保存する。ネットワークプロトコルは、例えば、TCP/IP、HTTP+XML(SOAP)などのどのような標準的なプロトコルを利用することもできる。もちろん、FTPやMAILなどのプロトコルを利用しても良い。

【0203】

複合機の動作は、アプリケーション3004により制御される。CPU3002は、アプリケーション3004からの指示に従って動作する。CPU3002は、ポリシーDB3003から蓄積されているポリシーを読み出す。そして、読み出したポリシーに記載されているルールに従って、複合機エンジン3001を制御し、そして、アプリケーション3004の指示を実現する。すなわち、ポリシーに記載されているルールに従って複合機3000の動作を制御する。

【0204】

次に、本発明の第4の実施例について説明する。図31は、本発明の第4の実施例を示す図である。図31は、取り外し可能な記憶媒体を通じて外部からポリシーを取得し、内部のポリシーDB（データターベース）に保存する複合機3000の実施例である。図31に示す複合機3000は、上述した、読取装置、印刷装置又は、複写装置又は、これらの組合せの複合機を構成する。複合機3000は、複合機エンジン3001、CPU（中央処理装置）3002、ポリシーDB3003、アプリケーション3004及び取り外し可能な記憶媒体3101により構成される。図31において、CPU3002は、アプリケーション300

4に指示に従って、取り外し可能な記憶媒体3101に記憶されているセキュリティポリシーを読み出して、内部のポリシーDB3003に保存する。内部のポリシーDB3003にセキュリティポリシーが記憶された後の動作は、上述の第3の実施例と同様である。

【0205】

取り外し可能な記憶媒体3101の例は、メモ리카ード、フレキシブルディスク、光ディスクなどのような標準的な記憶媒体を使用することができる。

【0206】

次に、本発明の第5の実施例について説明する。図32は、本発明の第5の実施例を示す。図32は、複合機3000に、ネットワーク3006を介して、セキュリティポリシーを設定するシステム3200の実施例を示す。図32に示すシステムは、複合機3000、ネットワーク3006、管理コンソール3201及びポリシー管理服务3202から構成される。

【0207】

先ず最初に、セキュリティポリシーを設定するシステム3200の管理者は、管理コンソール3201からポリシー管理服务3202へポリシーを設定する。

【0208】

次に、ポリシー管理服务3202は、複合機3000へネットワーク3006を介して設定されたポリシーを送信する。

【0209】

そして、複合機3000は、ネットワーク3006を介してポリシー管理服务3202から受信したポリシーに従って動作する。

【0210】

このような構成の場合に、複合機3000は、ポリシーを送信するポリシー管理服务3202が信頼できるものであるかどうかを確かめることで、間違ったポリシーの受信や悪意あるポリシーの設定などを防ぐこともできる。すなわち、ポリシー管理服务3202がポリシーの配布をする時に、以下のような動作を実行する。

【0211】

先ず最初に、ポリシー管理サービス 3202 は、自分自身の認証情報とポリシーを複合機 3000 に送信する。

【0212】

次に、複合機 3000 は送信されたポリシー管理サービス 3202 の認証情報を検証する。

【0213】

そして、このポリシー管理サービス 3202 の認証情報が正しいと確認された場合には、送信されたポリシーを正式なものとして利用する。

【0214】

このような動作を実行することにより、複合機 3000 は、間違ったポリシーの受信や悪意あるポリシーの設定などを防ぐこともできる。

【0215】

次に、本発明の第 6 の実施例について説明する。図 33 は、本発明の第 6 の実施例を示す。本実施例は、複合機を、最初にネットワークに接続した場合などのように、まだセキュリティポリシーを持っていない場合の複合機の動作の実施例を示す。

【0216】

図 33 に示すシステム 3200 は、複合機 3000 に、ネットワーク 3006 を介して、セキュリティポリシーを設定するシステム 3200 の実施例を示す。図 33 に示すシステムは、複合機 3000、ネットワーク 3006、管理コンソール 3201 及びポリシー管理サービス 3202 から構成される。本実施例は、以下のように実行される。

【0217】

先ず最初に、複合機 3000 の電源が投入される。

【0218】

次に、複合機 3000 はポリシー管理サービス 3202 からポリシーを取得する。

【0219】

そして、複合機 3000 は、ポリシー管理サービス 3202 取得したポリシーに従って動作する。

【0220】

このような場合には、ポリシーを受信する複合機 3000 が信頼できるものであるかどうかを確かめることで余分な情報の漏洩(ここではポリシー)を防ぐこともできる。すなわち、複合機 3000 が最初に、ポリシー管理サービス 3202 からポリシーを取得をする時に、以下のような動作を実行する。

【0221】

先ず最初に、複合機 3000 は、自分自身の認証情報とポリシーの取得要求をポリシー管理サービス 3202 に送信する。

【0222】

次に、ポリシー管理サービス 3202 は、送信された複合機 3000 の認証情報を検証する。

【0223】

そして、この複合機 3000 の認証情報が正しいと、ポリシー管理サービス 3202 が確認した場合には、複合機 3000 にポリシーを送信する。

このような動作を実行することにより、ポリシー管理サービス 3202 は、余分な情報の漏洩(ここではポリシー)を防ぐこともできる。

【0224】

次に、本発明の第 7 の実施例について説明する。図 34 は、本発明の第 7 の実施例を示す。本実施例は、上述の第 5 の実施例と第 6 の実施例に示すように、ポリシーを配布する及び、ポリシーを取得するというような、2 通りの動作を実現するためには、ポリシー管理サービス 3202 側と、複合機 3000 側に、2 通りのネットワークアプリケーションを用意する必要がある。本実施例では、このような 2 つの動作を、一つのアプリケーションで行うことができる。

【0225】

図 34 に示すシステム 3200 は、複合機 3000、ネットワーク 3006、管理コンソール 3201 及びポリシー管理サービス 3202 から構成される。

【0226】

本実施例の動作を以下に説明する。

【0227】

先ず最初に、システム3200の管理者は、管理コンソール3201からポリシー管理サービス3202へポリシーを設定する。

【0228】

次に、ポリシー管理サービス3202は、ポリシー配布通知を複合機3000へ送信する。

【0229】

そして、複合機3000は、ポリシー管理サービス3202からポリシーを取得する。

【0230】

最後に、複合機3000は、取得したポリシーに従って動作する。

【0231】

以上のように、このような2つの動作を、一つのアプリケーションで行うことができる。

【0232】

次に、本発明の第8の実施例について説明する。図35は、本発明の第8の実施例を示す。本実施例は、頻繁に電源を切断又は再投入する場合には、前述の実施例のように、その度に、複合機3000がポリシー管理サービス3202からポリシーを取得していたのでは、効率が悪い場合がある。そのような場合には、以下のように実行することができる。

【0233】

図35に示すシステム3200は、複合機3000、ネットワーク3006、管理コンソール3201、ポリシー管理サービス3202及び、複合機3000に内蔵又は、接続されたタイマー装置3501から構成される。

【0234】

第1のステップでは、最初に、複合機3000の内部に、ポリシーを取得する時間間隔(あるいは取得時刻)を予め設定する。

【0235】

そして、第1のステップでは、更に、複合機3000の通電中に、タイマー装置3501が、設定時刻の経過を検知する。

【0236】

第2のステップでは、第1のステップで検知された設定時刻に、複合機3000は、ポリシー管理サービス3202からポリシーを取得する。

【0237】

そして、第3のステップで、複合機3000は、取得したポリシーに従って動作する。

【0238】

このように、動作することにより、設定時刻において、複合機3000は、ポリシー管理サービス3202からポリシーを取得するので、電源の再投入の度に、ポリシーを取得することではなく、これにより、効率を向上することができる。

【0239】

次に、本発明の第9の実施例について説明する。図36は、本発明の第9の実施例を示す。本実施例は、ポリシーのサイズや回線の速度に依存して、ポリシーをオフラインで設定する場合の実施例を示す。

【0240】

本実施例では、先ず最初に、オフラインで、複合機3000に、ポリシーを設定する。

【0241】

次に、複合機3000は設定されたポリシーに従って動作する。

【0242】

オフラインでポリシーを設定する場合には、それに応じたオフラインメディアのI/F（インターフェース）を複合機に設ける。また、オフラインでポリシーを設定する場合には、そのポリシーに、改ざん検知コードなどを追加することにより、ポリシーの信頼性を向上することもできる。

【0243】

次に、本発明の第10の実施例について説明する。図37は、本発明の第10の実施例を示す。本実施例は、オフラインで設定したポリシーを切り替えて利用

する場合の実施例を示す。

【0244】

図37に示すシステム3200は、複合機3000、ネットワーク3006、管理コンソール3201及びポリシー管理サービス3202から構成される。

【0245】

先ず最初に、オフラインで、複合機3000に、1つ以上のポリシーを予め設定する。

【0246】

次に、管理コンソール3201から、ポリシー管理サービス3202に、ポリシーを設定する。

【0247】

そして、次に、ポリシー管理サービス3202は、複合機3000に、設定されたポリシーの選択情報を通知する。

【0248】

最後に、複合機3000は、ポリシー管理サービス3202により通知された、選択されたポリシーに従って動作する。

【0249】

本実施例により、オフラインで設定したポリシーを切り替えて利用することができる。

【0250】

【発明の効果】

以上説明したように、本発明によって、セキュリティポリシーに基づいた文書の読み取り装置、読み取り方法、ネットワーク配信を行う装置及びネットワーク配信を行う方法、その方法を実行するプログラム、そのプログラムを記憶した記憶媒体、伝送装置及び、セキュリティポリシーを外部から設定する入出力装置を提供することができる。

【図面の簡単な説明】

【図1】

セキュリティポリシーの例を示す図である。

【図 2】

document_label_terminology.xmlのファイルのリストの例を示す図である。

【図 3】

policy_terminology.xmlのファイルのリストの例を示す図（1）である。

【図 4】

policy_terminology.xmlのファイルのリストの例を示す図（2）である。

【図 5】

policy_terminology.xmlのファイルのリストの例を示す図（3）である。

【図 6】

policy_terminology.xmlのファイルのリストの例を示す図（4）である。

【図 7】

policy_terminology.xmlのファイルのリストの例を示す図（5）である。

【図 8】

policy_terminology.xmlのファイルのリストの例を示す図（6）である。

【図 9】

policy_terminology.xmlのファイルのリストの例を示す図（7）である。

【図 10】

policy_terminology.xmlのファイルのリストの例を示す図（8）である。

【図 11】

policy_terminology.xmlのファイルのリストの例を示す図（9）である。

【図 12】

policy_terminology.xmlのファイルのリストの例を示す図（10）である。

【図 13】

policy_terminology.xmlのファイルのリストの例を示す図（11）である。

【図 14】

policy.xmlのファイルのリストの例を示す図（1）である。

【図 15】

policy.xmlのファイルのリストの例を示す図（2）である。

【図 16】

policy.xmlのファイルのリストの例を示す図(3)である。

【図17】

policy.xmlのファイルのリストの例を示す図(4)である。

【図18】

policy.xmlのファイルのリストの例を示す図(5)である。

【図19】

policy.xmlのファイルのリストの例を示す図(6)である。

【図20】

policy.xmlのファイルのリストの例を示す図(7)である。

【図21】

policy.xmlのファイルのリストの例を示す図(8)である。

【図22】

policy.xmlのファイルのリストの例を示す図(9)である。

【図23】

policy.xmlのファイルのリストの例を示す図(10)である。

【図24】

DSPの識別情報の例を示す図である。

【図25】

ポリシーの内容を示す一実施例を示す図である。

【図26】

本発明のDSPの別の記述形式の実施例を示す図である。

【図27】

DSPを蓄積し且つ配布する種々の媒体を示す図である。

【図28】

本発明の実施例の文書読み取り装置の構成を示す図である。

【図29】

XML (E x t e n s i b l e M a r k u p L a n g u a g e) により記述した、本発明の実施例のセキュリティポリシーを示す図である。

【図30】

本発明の第3の実施例を示す図である。

【図31】

本発明の第4の実施例を示す図である。

【図32】

本発明の第5の実施例を示す図である。

【図33】

本発明の第6の実施例を示す図である。

【図34】

本発明の第7の実施例を示す図である。

【図35】

本発明の第8の実施例を示す図である。

【図36】

本発明の第9の実施例を示す図である。

【図37】

本発明の第10の実施例を示す図である。

【符号の説明】

- 50 DSP
- 51 ハードディスク
- 52 光磁気ディスク
- 53 フレキシブルディスク
- 54 光ディスク
- 55 コンピュータ
- 56 ネットワーク
- 100 文書読み取り装置
- 101 オペレーションパネル
- 102 データベース
- 103 ユーザ属性取得手段
- 104 文書属性取得手段
- 105 セキュリティーポリシー

- 1 0 6 読み取り手段
- 1 0 7 読み取りデータ
- 1 0 8 ネットワークポート
- 1 1 0 読み取り指示
- 3 0 0 0 複合機
- 3 0 0 1 複合機エンジン
- 3 0 0 2 C P U
- 3 0 0 3 ポリシーDB
- 3 0 0 4 アプリケーション
- 3 0 0 5 ネットワークポート
- 3 0 0 6 ネットワーク
- 3 2 0 1 管理コンソール
- 3 2 0 2 ポリシー管理サービス
- 3 5 0 1 タイマー装置

【書類名】

図面

【図1】

セキュリティポリシーの例を示す図

極秘文書について：

原則複写禁止（複写する際には管理責任者の許可を得なければならない）、
また、複写したことを記録しておかなければならない
プリントする際には複写禁止であることを示す透かしを入れなければならない、また、プリントしたことを記録しておかなければならない
閲覧は関係者のみ許可

丸秘文書について：

複写は関係者のみ許可
プリントする際には丸秘文書であることを示すラベルを同時に印刷しなければならない
閲覧は関係者のみ許可

社外秘文書について：

社外へ送付する際には管理責任者の許可を得なければならない
複写・プリント・閲覧は社内であれば許可不要

人事関連文書について：

すべて丸秘文書として扱う

【図 2】

document_label_terminology.xmlのファイルの
リストの例を示す図

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_label_terminology>
<about_this_terminology>
  <serial_number>RDST0100-000000000000001-
0001</serial_number>
  <title>Office System Research and Development Center,
DOCUMENT-LABEL-TERMINOLOGY</title>
  <version>1.00</version>
  <creation_date>2001/12/21 13:37:18</creation_date>
  <creator>Yoichi Kanai</creator>
  <description>This is a sample document-label
terminology.</description>
</about_this_terminology>
<enumeration>
  <enum_id>doc_category</enum_id>
  <enum_name>Document Category</enum_name>
  <description>文書カテゴリの種類</description>
  <item>
    <name>internal_doc</name>
    <description>社内一般文書</description>
  </item>
  <item>
    <name>human_resource_doc</name>
    <description>人事関連文書</description>
  </item>
  <item>
    <name>technical_doc</name>
    <description>技術関連文書</description>
  </item>
</enumeration>
<enumeration>
  <enum_id>doc_security_level</enum_id>
  <enum_name>Document Security Level</enum_name>
  <description>文書のセキュリティレベルの種類</description>
  <item>
    <name>basic</name>
    <description>社外秘</description>
  </item>
  <item>
    <name>meium</name>
    <description>秘</description>
  </item>
  <item>
    <name>high</name>
    <description>極秘</description>
  </item>
</enumeration>
</document_label_terminology>
```


【図 3】

policy_terminology.xmlのファイルのリストの例を示す図(1)

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<policy_terminology>
<about_this_terminology>
  <serial_number>RDST0100-00000000000001-
9487</serial_number>
  <title>Office System Research and Development Center,
DOCUMENT-SECURITY-POLICY-TERMINOLOGY</title>
  <version>1.00</version>
  <creation_date>2001/12/21 13:37:18</creation_date>
  <creator>Yoichi Kanai</creator>
  <description>This is a sample policy
terminology.</description>
</about_this_terminology>

<!-- システムタイプの列挙 -->
<enumeration>
  <enum_id>system_type</enum_id>
  <enum_name>System Type</enum name>
  <description>システムタイプの種類</description>
  <item>
    <name>Copier</name>
    <description>複写機</description>
    <operation>copier_operation</operation>
  </item>
  <item>
    <name>Printer</name>
    <description>プリンタ</description>
    <operation>printer_operation</operation>
  </item>
  <item>
    <name>Facsimile</name>
    <description>ファクシミリ</description>
    <operation>fax_operation</operation>
  </item>
  <item>
    <name>Scanner</name>
    <description>スキャナ</description>
    <operation>scanner_operation</operation>
  </item>
  <item>
    <name>Document Repository</name>
    <description>文書リポジトリ</description>
    <operation>repository_operation</operation>
  </item>
  <item>
    <name>E-Meeting</name>
    <description>電子会議システム</description>
    <operation>emeeting_operation</operation>
```

【図 4】

policy_terminology.xmlのファイルのリストの例を示す図(2)

```
</item>
</enumeration>
<!-- システムタイプごとのオペレーションの列挙 -->
<enumeration>
  <enum_id>copier_operation</enum_id>
  <enum_name>Copier Operation</enum_name>
  <description>複写機に関わるオペレーション</description>
  <item>
    <name>hardcopy</name>
    <description>紙から紙への複写</description>
    <requirement>hardcopy_requirement</requirement>
  </item>
</enumeration>
<enumeration>
  <enum_id>printer_operation</enum_id>
  <enum_name>Printer Operation</enum_name>
  <description>プリンタに関わるオペレーション</description>
  <item>
    <name>print</name>
    <description>電子文書を紙へ印刷</description>
    <requirement>print_requirement</requirement>
  </item>
</enumeration>
<enumeration>
  <enum_id>fax_operation</enum_id>
  <enum_name>Facsimile Operation</enum_name>
  <description>ファクスに関わるオペレーション</description>
  <item>
    <name>fax_send</name>
    <description>ファクスの送信</description>
    <requirement>fax_send_requirement</requirement>
  </item>
  <item>
    <name>fax_receive</name>
    <description>ファクスの受信</description>
    <requirement>fax_receive_requirement</requirement>
  </item>
</enumeration>
<enumeration>
  <enum_id>scanner_operation</enum_id>
  <enum_name>Scanner Operation</enum_name>
  <description>スキャナに関わるオペレーション</description>
  <item>
    <name>scan</name>
    <description>紙文書をスキャンして電子文書にする</description>
    <requirement>scan_requirement</requirement>
  </item>
</enumeration>
```

【図 5】

policy_terminology.xmlのファイルのリストの例を示す図(3)

```
<enumeration>
  <enum_id>repository_operation</enum_id>
  <enum_name>Document Repository Operation</enum_name>
  <description>文書リポジトリに関わるオペレーション
</description>
  <item>
    <name>store</name>
    <description>保存する</description>
    <requirement>store_requirement</requirement>
  </item>
  <item>
    <name>revise</name>
    <description>改訂・編集する</description>
    <requirement>revise_requirement</requirement>
  </item>
  <item>
    <name>delete</name>
    <description>削除・破棄する</description>
    <requirement>delete_requirement</requirement>
  </item>
  <item>
    <name>read</name>
    <description>参照する</description>
    <requirement>read_requirement</requirement>
  </item>
  <item>
    <name>net_delivery</name>
    <description>ネットワークで配布する（送信する）
  </description>
    <requirement>net_delivery_requirement</requirement>
  </item>
  <item>
    <name>disc_delivery</name>
    <description>ディスクで配布する（送付する）
  </description>
    <requirement>disc_delivery_requirement</requirement>
  </item>
  <item>
    <name>archive</name>
    <description>アーカイブ・バックアップする
  </description>
    <requirement>archive_requirement</requirement>
  </item>
</enumeration>
<enumeration>
  <enum_id>emeeting_operation</enum_id>
  <enum_name>E-Meeting Operation</enum_name>
  <description>電子会議システムに関わるオペレーション
</description>
```

【図 6】

policy_terminology.xmlのファイルのリストの例を示す図(4)

```

<item>
  <name>meeting_use</name>
  <description>会議で利用する</description>

  <requirement>meeting_use_requirement</requirement>
</item>
</enumeration>

<!-- オペレーションごとに適用できる要件の列挙 -->
<!-- ユーザ認証, 文書識別, アクセス制御 (利用制限) は基本メカニズムとし
て提供されるため, 要件には含めない -->
<enumeration>
  <enum_id>hardcopy_requirement</enum_id>
  <enum_name>Hardcopy Requirement</enum_name>
  <description>複写に関わる要件</description>
  <item>
    <name>explicit authorization</name>
    <description>明示的な許可</description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証跡のイメージ付き記録
  </description>
  </item>
</enumeration>
<enumeration>
  <enum_id>print_requirement</enum_id>
  <enum_name>Print Requirement</enum_name>
  <description>印刷に関わる要件</description>
  <item>
    <name>explicit authorization</name>
    <description>明示的な許可 (利用制限) </description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証跡のイメージ付き記録
  </description>
  </item>
  <item>
    <name>private_access</name>
    <description>プリントした本人による紙出力
  </description>
  </item>

```

【図 7】

policy_terminology.xmlのファイルのリストの例を示す図(5)

```

    <item>
      <name>trusted_channel</name>
      <description>信頼チャネルの利用 (印刷データの暗号化)
    </description>
    </item>
    <item>
      <name>embed_trace_info</name>
      <description>プリントアウトに追跡情報埋め込み (透かし,
ラベル, バーコード) </description>
    </item>
  </enumeration>
  <enumeration>
    <enum_id>fax_send_requirement</enum_id>
    <enum_name>Requirement on Sending Fax
Message</enum_name>
    <description>ファクス送信に関わる要件</description>
    <item>
      <name>explicit_authorization</name>
      <description>明示的な許可 (利用制限) </description>
    </item>
    <item>
      <name>audit</name>
      <description>監査証跡の記録</description>
    </item>
    <item>
      <name>audit_with_image</name>
      <description>監査証跡のイメージ付き記録
    </description>
    </item>
    <item>
      <name>destination_restriction</name>
      <description>宛先制限</description>
    </item>
    <item>
      <name>private_mode</name>
      <description>親展モードでの送信</description>
    </item>
    <item>
      <name>trusted_channel</name>
      <description>信頼チャネルの利用 (ファクスデータの暗号
化) </description>
    </item>
    <item>
      <name>embed_trace_info</name>
      <description>送信ファクスに追跡情報埋め込み (透かし, ラ
ベル, バーコード) </description>
    </item>
    <item>
      <name>non_repudiation</name>
      <description>否認防止 (受取証の取得) </description>
    </item>
  </enumeration>

```

【図 8】

policy_terminology.xmlのファイルのリストの例を示す図(6)

```

</enumeration>
<enumeration>
  <enum_id>fax_receive_requirement</enum_id>
  <enum_name>Requirement on Receiving Fax
  Message</enum_name>
  <description>ファクス受信に関わる要件</description>
  <item>
    <name>audit</name>
    <description>監査証拠の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証拠のイメージ付き記録
  </description>
  </item>
  <item>
    <name>private_access</name>
    <description>親展ファクスの宛先本人による取り出し
  </description>
  </item>
  <item>
    <name>trusted_timestamp</name>
    <description>信頼タイムスタンプ</description>
  </item>
  <item>
    <name>embed_trace_info</name>
    <description>受信ファクスに追跡情報埋め込み (透かし, ラ
    ベル, バーコード) </description>
  </item>
</enumeration>
<enumeration>
  <enum_id>scan_requirement</enum_id>
  <enum_name>Scan Requirement</enum_name>
  <description>スキャンに関わる要件 (保存した後については保存要件
  を適用する) </description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可 (利用制限) </description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証拠の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証拠のイメージ付き記録
  </description>
  </item>
  <item>
    <name>embed_trace_info</name>
    <description>スキャン画像に追跡情報埋め込み (透かし, ラ

```

【図 9】

policy_terminology.xmlのファイルのリストの例を示す図(7)

```

ベル, バーコード) </description>
</item>
</enumeration>
<enumeration>
  <enum_id>store_requirement</enum_id>
  <enum_name>Store Requirement</enum_name>
  <description>保存に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可 (利用制限) </description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証拠の記録</description>
  </item>
  <item>
    <name>encryption</name>
    <description>保存データの暗号化</description>
  </item>
  <item>
    <name>integrity_protection</name>
    <description>保存データの改ざん保護</description>
  </item>
</enumeration>
<enumeration>
  <enum_id>revise_requirement</enum_id>
  <enum_name>Revise Requirement</enum_name>
  <description>改訂に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可 (利用制限) </description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証拠の記録</description>
  </item>
  <item>
    <name>versioning</name>
    <description>バージョン管理</description>
  </item>
</enumeration>
<enumeration>
  <enum_id>delete_requirement</enum_id>
  <enum_name>Delete Requirement</enum_name>
  <description>削除・破棄に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可 (利用制限) </description>
  </item>
  <item>
    <name>audit</name>

```

【図 10】

policy_terminology.xmlのファイルのリストの例を示す図(8)

```

        <description>監査証跡の記録</description>
      </item>
      <item>
        <name>audit_with_image</name>
        <description>監査証跡のイメージ付き記録</description>
      </item>
    </enumeration>
    <enumeration>
      <enum_id>complete_erase</enum_id>
      <enum_name>Complete Erase</enum_name>
      <description>完全消去</description>
    </enumeration>
    <enum_id>read_requirement</enum_id>
    <enum_name>Read Requirement</enum_name>
    <description>参照に関わる要件</description>
    <item>
      <name>explicit_authorization</name>
      <description>明示的な許可 (利用制限)</description>
    </item>
    <item>
      <name>audit</name>
      <description>監査証跡の記録</description>
    </item>
    <item>
      <name>edit_restriction</name>
      <description>編集禁止のデータのみ参照許可</description>
    </item>
    <item>
      <name>print_restriction</name>
      <description>印刷禁止のデータのみ参照許可</description>
    </item>
    <item>
      <name>location_restriction</name>
      <description>参照場所限定のデータのみ参照許可</description>
    </item>
    <item>
      <name>user_restriction</name>
      <description>ユーザ限定のデータのみ参照許可</description>
    </item>
  </enumeration>
  <enum_id>net_delivery_requirement</enum_id>
  <enum_name>Delivery via Network Requirement</enum_name>
  <description>ネットワーク配信 (送信) に関わる要件</description>
  <item>

```


【図 11】

policy_terminology.xmlのファイルのリストの例を示す図(9)

```

        <name>explicit_authorization</name>
        <description>明示的な許可 (利用制限) </description>
    </item>
    <item>
        <name>audit</name>
        <description>監査証拠の記録</description>
    </item>
    <item>
        <name>audit_with_image</name>
        <description>監査証拠のイメージ付き記録
    </description>
    </item>
    <item>
        <name>trusted_channel</name>
        <description>信頼チャネルの利用 (送信データの暗号化)
    </description>
    </item>
    <item>
        <name>destination_restriction</name>
        <description>宛先制限 (社内のみ配信可能など)
    </description>
    </item>
    <item>
        <name>edit_restriction</name>
        <description>編集禁止のデータのみ配信許可
    </description>
    </item>
    <item>
        <name>print_restriction</name>
        <description>印刷禁止のデータのみ配信許可
    </description>
    </item>
    <item>
        <name>location_restriction</name>
        <description>参照場所限定のデータのみ配信許可
    </description>
    </item>
    <item>
        <name>user_restriction</name>
        <description>ユーザ限定のデータのみ配信許可
    </description>
    </item>
</enumeration>
<enumeration>
    <enum_id>disc_delivery_requirement</enum_id>
    <enum_name>Delivery via Disc Requirement</enum_name>
    <description>ディスク配布 (送付) に関わる要件</description>
    <item>
        <name>explicit_authorization</name>
        <description>明示的な許可 (利用制限) </description>
    </item>

```

【図 12】

policy_terminology.xmlのファイルのリストの例を示す図(10)

```

<item>
  <name>audit</name>
  <description>監査証跡の記録</description>
</item>
<item>
  <name>audit_with_image</name>
  <description>監査証跡のイメージ付き記録</description>
</item>
<item>
  <name>encryption</name>
  <description>送付データの暗号化</description>
</item>
<item>
  <name>integrity_protection</name>
  <description>送付データの改ざん保護</description>
</item>
<item>
  <name>edit_restriction</name>
  <description>編集禁止のデータのみ送付許可</description>
</item>
<item>
  <name>print_restriction</name>
  <description>印刷禁止のデータのみ送付許可</description>
</item>
<item>
  <name>location_restriction</name>
  <description>参照場所限定のデータのみ送付許可</description>
</item>
<item>
  <name>user_restriction</name>
  <description>ユーザ限定のデータのみ送付許可</description>
</item>
</enumeration>
<enumeration>
  <enum_id>archive_requirement</enum_id>
  <enum_name>Archive Requirement</enum_name>
  <description>アーカイブ・バックアップに関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可(利用制限)</description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証跡の記録</description>
  </item>
</enumeration>

```

【図 13】

policy_terminology.xmlのファイルのリストの例を示す図(11)

```
<item>
  <name>encryption</name>
  <description>アーカイブデータの暗号化</description>
</item>
<item>
  <name>integrity_protection</name>
  <description>アーカイブデータの改ざん保護
</description>
</item>
</enumeration>
<enumeration>
  <enum_id>meeting_use_requirement</enum_id>
  <enum_name>Meeting-use Requirement</enum_name>
  <description>会議での利用に関わる要件</description>
  <item>
    <name>explicit_authorization</name>
    <description>明示的な許可 (利用制限) </description>
  </item>
  <item>
    <name>audit</name>
    <description>監査証拠の記録</description>
  </item>
  <item>
    <name>audit_with_image</name>
    <description>監査証拠のイメージ付き記録
</description>
  </item>
</enumeration>
</policy_terminology>
```

【図 14】

policy.xmlのファイルのリストの例を示す図(1)

```
<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_security_policy>
<about_this_policy>
  <serial_number>RDSP0100-000000000000012-
2023</serial_number>
  <terminology_applied>RDST0100-00000000000001-
9487</terminology_applied>
  <title>Office System Research and Development Center,
DOCUMENT-SECURITY-POLICY</title>
  <version>1.30</version>
  <creation_date>2002/02/18 22:30:24</creation_date>
  <creator>Yoichi Kanai</creator>
  <description>This is a sample document security
policy.</description>
</about_this_policy>
<policy>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>basic</doc_security_level>
    <acl>
      <ace>
        <user_category>ANY</user_category>
        <user_security_level>ANY</user_security_level>
        <operation>
          <name>hardcopy</name>
          <allowed/><!-- allowed
without any requirement -->
        </operation>
        <operation>
          <name>print</name>
          <allowed/><!-- allowed
without any requirement -->
        </operation>
        <operation>
          <name>fax_send</name>
          <allowed/><!-- allowed
without any requirement -->
        </operation>
        <operation>
          <name>fax_receive</name>
          <allowed/><!-- allowed
without any requirement -->
        </operation>
        <operation>
          <name>scan</name>
          <allowed/><!-- allowed
```

【図 15】

policy.xmlのファイルのリストの例を示す図(2)

```

                                <allowed/><!--      allowed
without any requirement -->
                                </operation>
                                <operation>
                                <name>store</name>
                                <allowed/><!--      allowed
without any requirement -->
                                </operation>
                                <operation>
                                <name>revise</name>
                                <allowed/><!--      allowed
without any requirement -->
                                </operation>
                                <operation>
                                <name>delete</name>
                                <allowed/><!--      allowed
without any requirement -->
                                </operation>
                                <operation>
                                <name>read</name>
                                <allowed/><!--      allowed
without any requirement -->
                                </operation>
                                <operation>
                                <name>net_delivery</name>

                                <requirement>audit</requirement>

                                <requirement>explicit_authorization</requirement>

                                <requirement>print_restriction</requirement>

                                <requirement>trusted_channel</requirement>
                                </operation>
                                <operation>
                                <name>disc_delivery</name>

                                <requirement>audit</requirement>

                                <requirement>explicit_authorization</requirement>

                                <requirement>print_restriction</requirement>
                                </operation>
                                <operation>
                                <name>archive</name>
                                <allowed/><!--      allowed
without any requirement -->
                                </operation>
                                <operation>
                                <name>meeting_use</name>
                                <allowed/><!--      allowed

```

【図 16】

policy.xmlのファイルのリストの例を示す図(3)

```

without any requirement -->
    </operation>
    </ace>
    </acl>
</acc_rule>
<acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>medium</doc_security_level>
    <acl>
        <ace>
            <user_category>DOC-
CATEGORY</user_category>
            <user_security_level>ANY</user_security_level>
            <operation>
                <name>hardcopy</name>
            </operation>
            <requirement>audit</requirement>
            <requirement>embed_trace_info</requirement>
            </operation>
            <operation>
                <name>print</name>
            </operation>
            <requirement>audit</requirement>
            <requirement>embed_trace_info</requirement>
            </operation>
            <operation>
                <name>fax_send</name>
                <denied/><!-- denied even if
it is explicitly authorized -->
            </operation>
            <operation>
                <name>fax_receive</name>
                <allowed/><!-- allowed
without any requirement -->
            </operation>
            <operation>
                <name>scan</name>
            </operation>
            <requirement>audit</requirement>
            <requirement>embed_trace_info</requirement>
            </operation>
            <operation>
                <name>store</name>
                <allowed/><!-- allowed
without any requirement -->
            </operation>
            <operation>

```

【図 17】

policy.xmlのファイルのリストの例を示す図(4)

```

                                <name>revise</name>
                                <allowed/><!--          allowed
without any requirement -->
                                </operation>
                                <operation>
                                <name>delete</name>
                                <allowed/><!--          allowed
without any requirement -->
                                </operation>
                                <operation>
                                <name>read</name>

                                <requirement>audit</requirement>

                                <requirement>print_restriction</requirement>

                                <requirement>location_restriction</requirement>
                                </operation>
                                <operation>
                                <name>net_delivery</name>

                                <requirement>audit</requirement>

                                <requirement>explicit_authorization</requirement>

                                <requirement>print_restriction</requirement>

                                <requirement>trusted_channel</requirement>
                                </operation>
                                <operation>
                                <name>disc_delivery</name>

                                <requirement>audit</requirement>

                                <requirement>explicit_authorization</requirement>

                                <requirement>print_restriction</requirement>
                                </operation>
                                <operation>
                                <name>archive</name>
                                <allowed/><!--          allowed
without any requirement -->
                                </operation>
                                <operation>
                                <name>meeting_use</name>
                                <allowed/><!--          allowed
without any requirement -->
                                </operation>
                                </ace>
                                <ace>
                                <user_category>ANY</user_category>

```

【図 18】

policy.xmlのファイルのリストの例を示す図(5)

```
<user_security_level>ANY</user_security_level>
  <operation>
    <name>hardcopy</name>
    <denied/><!-- denied even if
it is explicitly authorized -->
  </operation>
  <operation>
    <name>print</name>
    <denied/><!-- denied even if
it is explicitly authorized -->
  </operation>
  <operation>
    <name>fax_send</name>
    <denied/><!-- denied even if
it is explicitly authorized -->
  </operation>
  <operation>
    <name>fax_receive</name>
    <denied/><!-- denied even if
it is explicitly authorized -->
  </operation>
  <operation>
    <name>scan</name>
    <denied/><!-- denied even if
it is explicitly authorized -->
  </operation>
  <operation>
    <name>store</name>
    <denied/><!-- denied even if
it is explicitly authorized -->
  </operation>
  <operation>
    <name>revise</name>
    <denied/><!-- denied even if
it is explicitly authorized -->
  </operation>
  <operation>
    <name>delete</name>
    <denied/><!-- denied even if
it is explicitly authorized -->
  </operation>
  <operation>
    <name>read</name>

<requirement>explicit_authorization</requirement>
<requirement>audit</requirement>
<requirement>print_restriction</requirement>
```


【図 19】

policy.xmlのファイルのリストの例を示す図(6)

```

<requirement>location_restriction</requirement>
    </operation>
    <operation>
        <name>net_delivery</name>
        <denied/><!-- denied even if
it is explicitly authorized -->
    </operation>
    <operation>
        <name>disc_delivery</name>
        <denied/><!-- denied even if
it is explicitly authorized -->
    </operation>
    <operation>
        <name>archive</name>
        <denied/><!-- denied even if
it is explicitly authorized -->
    </operation>
    <operation>
        <name>meeting_use</name>
        <denied/><!-- denied even if
it is explicitly authorized -->
    </operation>
    </ace>
    </acl>
</acc_rule>
<acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>high</doc_security_level>
    <acl>
        <ace>
            <user_category>DOC-
CATEGORY</user_category>
            <user_security_level>ANY</user_security_level>
            <operation>
                <name>hardcopy</name>
                <denied/><!-- denied even if
it is explicitly authorized -->
            </operation>
            <operation>
                <name>print</name>

<requirement>explicit_authorization</requirement>
<requirement>audit</requirement>
<requirement>private_access</requirement>
<requirement>trusted_channel</requirement>
<requirement>embed_trace_info</requirement>

```

【図 20】

policy.xmlのファイルのリストの例を示す図(7)

```

                                </operation>
                                <operation>
                                  <name>fax_send</name>
                                  <denied/><!-- denied even if
it is explicitly authorized -->
                                </operation>
                                <operation>
                                  <name>fax_receive</name>
                                  <allowed/><!--          allowed
without any requirement -->
                                </operation>
                                <operation>
                                  <name>scan</name>
                                  <denied/><!-- denied even if
it is explicitly authorized -->
                                </operation>
                                <operation>
                                  <name>store</name>

                                <requirement>audit</requirement>

                                <requirement>encryption</requirement>

                                <requirement>integrity_protection</requirement>
                                </operation>
                                <operation>
                                  <name>revise</name>

                                <requirement>versioning</requirement>
                                </operation>
                                <operation>
                                  <name>delete</name>

                                <requirement>complete_erase</requirement>
                                </operation>
                                <operation>
                                  <name>read</name>

                                <requirement>audit</requirement>

                                <requirement>print_restriction</requirement>

                                <requirement>location_restriction</requirement>

                                <requirement>user_restriction</requirement>
                                </operation>
                                <operation>
                                  <name>net_delivery</name>
                                  <denied/><!-- denied even if
it is explicitly authorized -->
                                </operation>

```

【図 21】

policy.xmlのファイルのリストの例を示す図(8)

```

        <operation>
            <name>disc_delivery</name>

        <requirement>audit</requirement>

        <requirement>explicit_authorization</requirement>

        <requirement>encryption</requirement>

        <requirement>print_restriction</requirement>
        </operation>
        <operation>
            <name>archive</name>

        <requirement>encryption</requirement>

        <requirement>integrity_protection</requirement>
        </operation>
        <operation>
            <name>meeting_use</name>

        <requirement>explicit_authorization</requirement>
        </operation>
    </ace>
    <ace>
        <user_category>ANY</user_category>

        <user_security_level>ANY</user_security_level>
        <operation>
            <name>hardcopy</name>
            <denied/><!-- denied even if
it is explicitly authorized -->
        </operation>
        <operation>
            <name>print</name>
            <denied/><!-- denied even if
it is explicitly authorized -->
        </operation>
        <operation>
            <name>fax_send</name>
            <denied/><!-- denied even if
it is explicitly authorized -->
        </operation>
        <operation>
            <name>fax_receive</name>
            <denied/><!-- denied even if
it is explicitly authorized -->
        </operation>
        <operation>
            <name>scan</name>
            <denied/><!-- denied even if

```

【図 22】

policy.xmlのファイルのリストの例を示す図(9)

```
it is explicitly authorized -->
    </operation>
    <operation>
        <name>store</name>
        <denied/><!-- denied even if
it is explicitly authorized -->
    </operation>
    <operation>
        <name>revise</name>
        <denied/><!-- denied even if
it is explicitly authorized -->
    </operation>
    <operation>
        <name>delete</name>
        <denied/><!-- denied even if
it is explicitly authorized -->
    </operation>
    <operation>
        <name>read</name>

    <requirement>explicit_authorization</requirement>

    <requirement>audit</requirement>

    <requirement>print_restriction</requirement>

    <requirement>location_restriction</requirement>

    <requirement>user_restriction</requirement>
    </operation>
    <operation>
        <name>net_delivery</name>
        <denied/><!-- denied even if
it is explicitly authorized -->
    </operation>
    <operation>
        <name>disc_delivery</name>
        <denied/><!-- denied even if
it is explicitly authorized -->
    </operation>
    <operation>
        <name>archive</name>
        <denied/><!-- denied even if
it is explicitly authorized -->
    </operation>
    <operation>
        <name>meeting_use</name>
        <denied/><!-- denied even if
it is explicitly authorized -->
    </operation>
</ace>
```

【図 23】

policy.xmlのファイルのリストの例を示す図(10)

```
        </acl>
      </acc_rule>
</policy>
</document security_policy>
```

【図 24】

DSPの識別情報の例を示す図

```
<about_this_policy>
  <serial_number>RDSP0100-00000000000012-2023</serial_number>
  <terminology_applied>RDST0100-00000000000001-
9487</terminology_applied>
  <title>Office System Research and Development Center,
DOCUMENT-SECURITY-POLICY</title>
  <version>1.20</version>
  <creation_date>2002/02/18 22:30:24</creation_date>
  <creator>Yoichi Kanai</creator>
  <description>This is a sample document security
policy.</description>
</about_this_policy>
```

【図 25】

ポリシーの内容を示す一実施例を示す図

```

<policy>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>medium</doc_security_level>
    <acl>
      <ace>
        <user_category>DOC-
CATEGORY</user_category>
        <user_security_level>ANY</user_security_level>
        <operation>
          <name>fax_send</name>
          <denied/><!-- denied even if it
is explicitly authorized -->
        </operation>
        <operation>
          <name>net_delivery</name>
        </operation>
        <requirement>audit</requirement>
        <requirement>explicit_authorization</requirement>
        ...
      </operation>
      <operation>
        <name>fax_receive</name>
        <allowed/><!-- allowed without
requirements -->
      </operation>
      ...
    </ace>
    <ace>
      ...
    </ace>
  </acl>
</acc_rule>
<acc_rule>
  <doc_category>ANY</doc_category>
  <doc_security_level>high</doc_security_level>
  <acl>
    ...
  </acl>
</acc_rule>
</policy>

```

【図 26】

本発明のDSPの別の記述形式の実施例を示す図

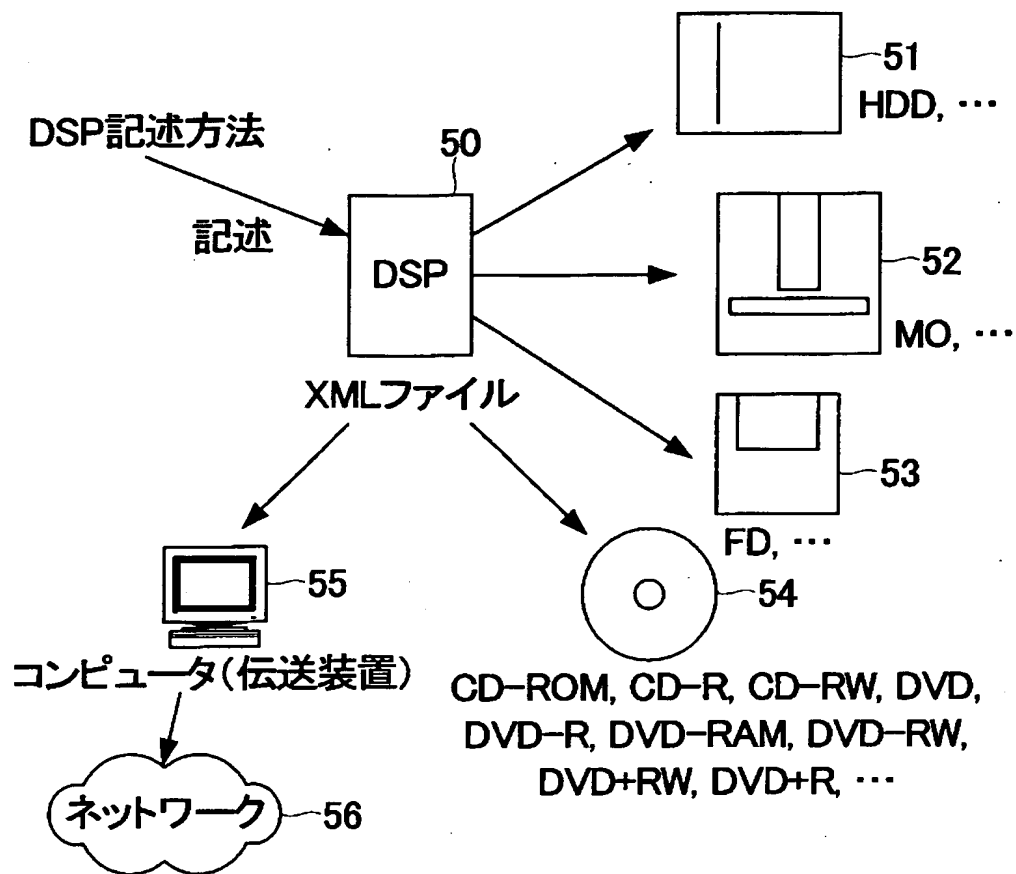
```

<policy>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>medium</doc_security_level>
    <acl>
      <ace>
        <user_category>DOC-
CATEGORY</user_category>
        <user_security_level>ANY</user_security_level>
        <denied_operations> <!-- denied even if
it is explicitly authorized -->
          <name>fax_send</name>
        </denied_operations>
        <operation>
          <name>net_delivery</name>
        </operation>
        <requirement>audit</requirement>
        <requirement>explicit_authorization</requirement>
        ...
      </ace>
      <ace>
        ...
        <operation>
          <name>fax_receive</name>
          <name>store</name>
        </operation>
        <allowed_operations> <!-- allowed
without requirements -->
          <name>fax_receive</name>
          <name>store</name>
        </allowed_operations>
      </ace>
    </ace>
  </acl>
</acc_rule>
<acc_rule>
  <doc_category>ANY</doc_category>
  <doc_security_level>high</doc_security_level>
  <acl>
    ...
  </acl>
</acc_rule>
</policy>

```

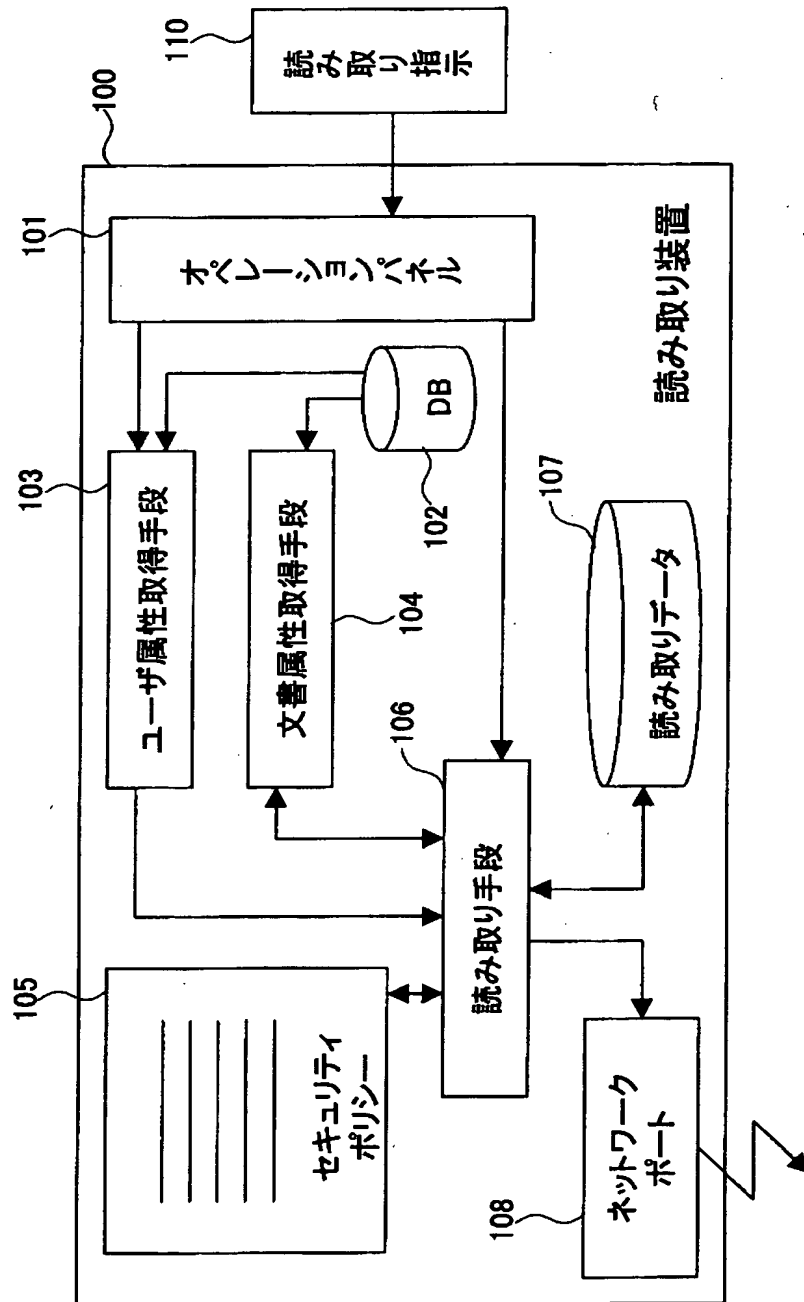
【図 27】

DSPを蓄積し且つ配布する種々の媒体を示す図



【図 28】

本発明の実施例の文書読み取り装置の構成を示す図



【図 29】

XML(Extensible Markup Language)により記述した 本発明の実施例のセキュリティポリシーを示す図

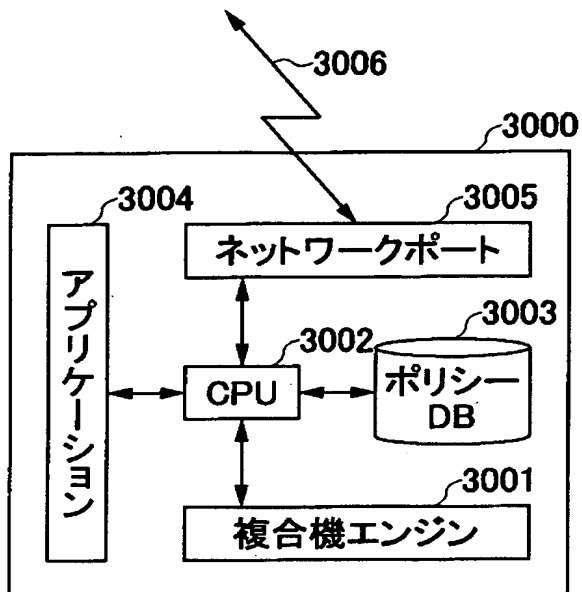
```

<?xml version="1.0" encoding="SHIFT-JIS" ?>
<document_security_policy>
<policy>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>basic</doc_security_level>
    <acl>
      <ace>
        <user_category>ANY</user_category>
        <user_security_level>ANY</user_security_level>
        <operation>
          <name>scan</name>
          <allowed/><!-- allowed without any requirement -->
        </operation>
        <operation>
          <name>net_delivery</name>
          <requirement>audit</requirement>
          <requirement>print_restriction</requirement>
          <requirement>trusted_channel</requirement>
        </operation>
      </ace>
    </acl>
  </acc_rule>
  <acc_rule>
    <doc_category>ANY</doc_category>
    <doc_security_level>high</doc_security_level>
    <acl>
      <ace>
        <user_category>DOC-CATEGORY</user_category>
        <user_security_level>ANY</user_security_level>
        <operation>
          <name>scan</name>
          <requirement>audit</requirement>
          <requirement>embed_trace_info</requirement>
        </operation>
      </ace>
    </acl>
  </acc_rule>
</policy>

```

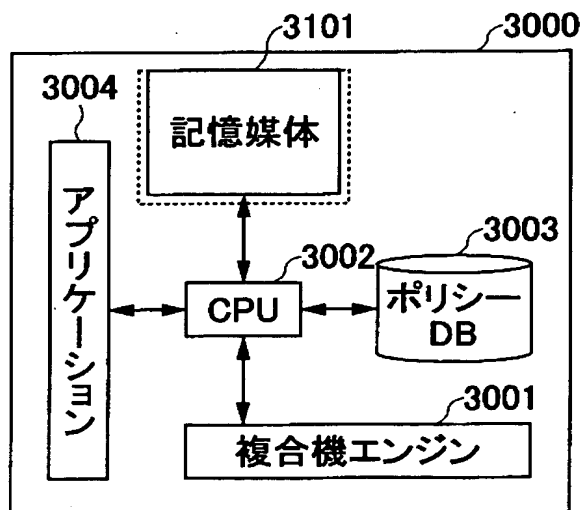
【図 30】

本発明の第3の実施例を示す図



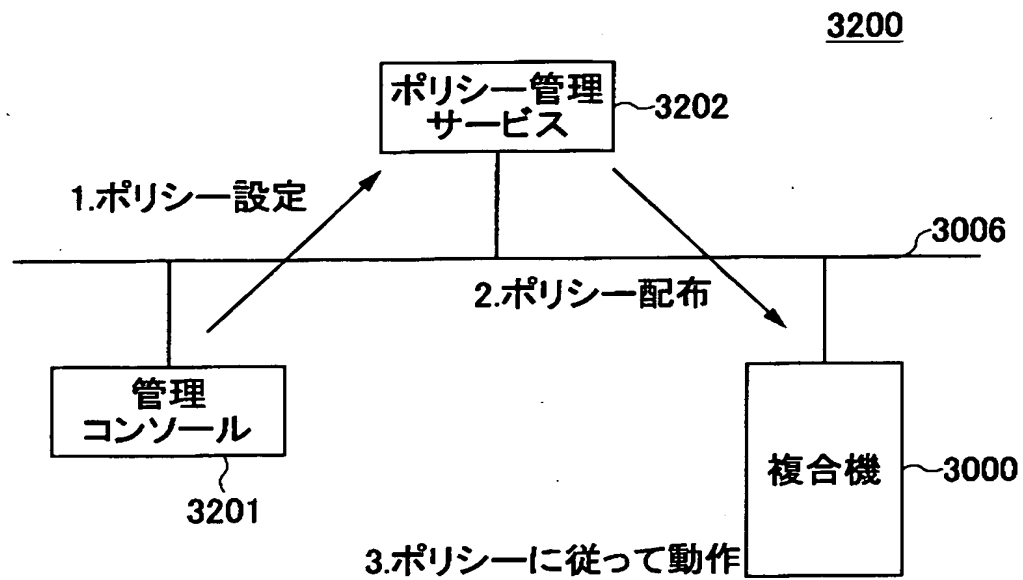
【図 31】

本発明の第4の実施例を示す図



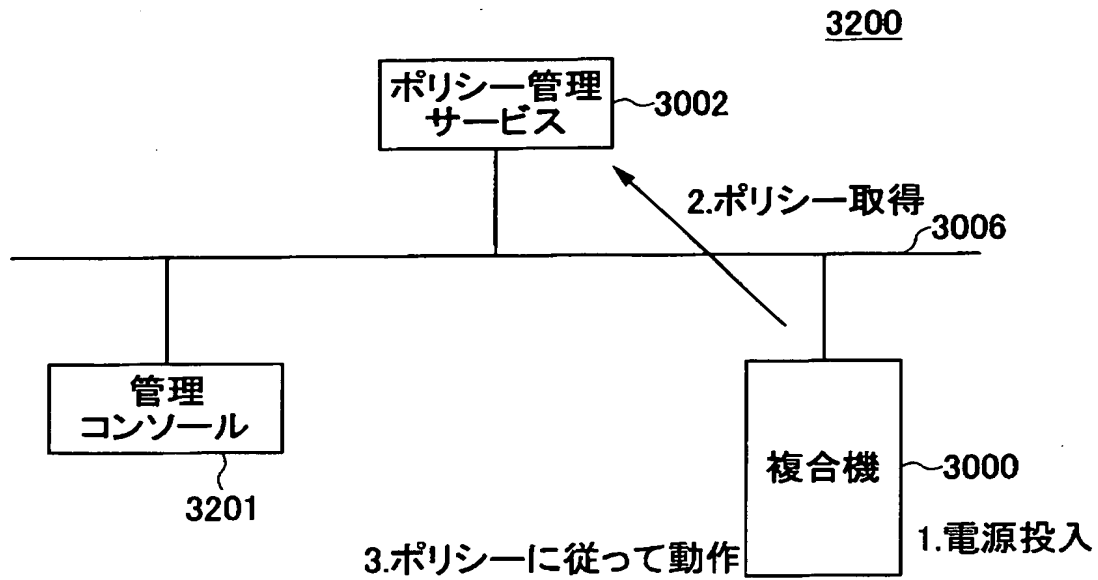
【図 3 2】

本発明の第5の実施例を示す図



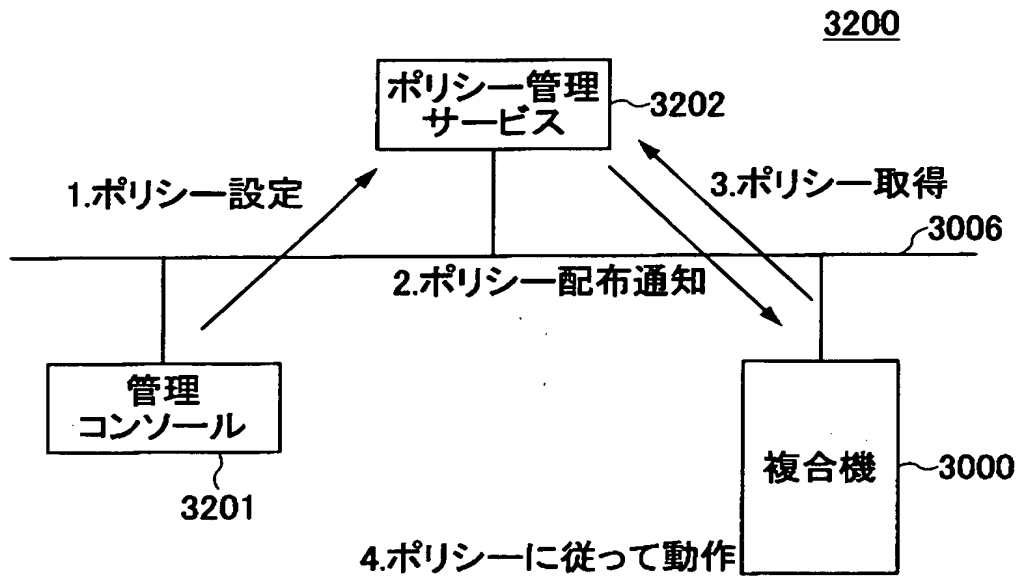
【図 33】

本発明の第6の実施例を示す図



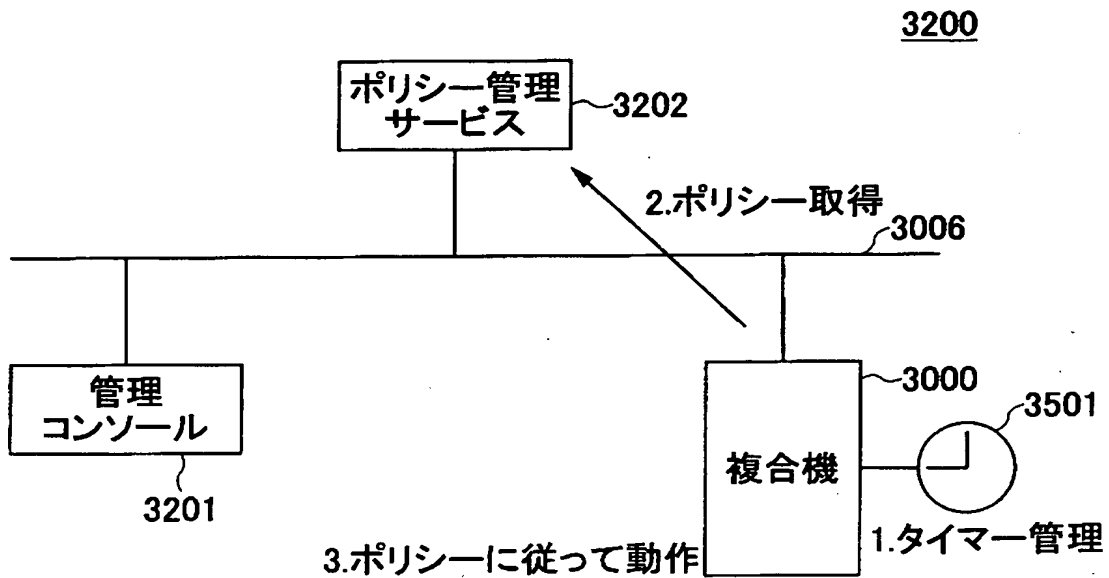
【図 34】

本発明の第7の実施例を示す図



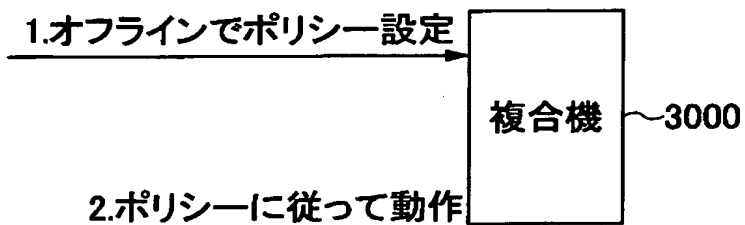
【図 3 5】

本発明の第8の実施例を示す図



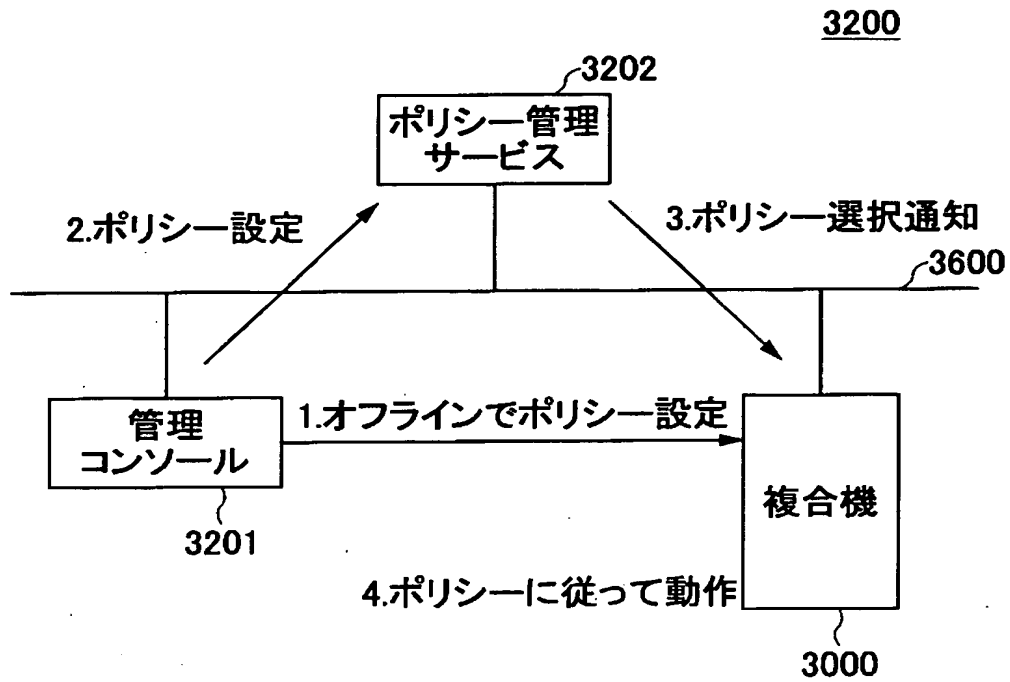
【図 3 6】

本発明の第9の実施例を示す図



【図 37】

本発明の第10の実施例を示す図



【書類名】 要約書

【要約】

【課題】 文書に関するセキュリティポリシーに基づいて、紙文書の読み取り、ネットワークへの配信を行う方法を提供する。

【解決手段】 ユーザ属性を取得し、文書属性を取得し、ユーザ属性と文書属性との組み合わせに対して読み取りが許可されているかをセキュリティポリシーにより判断し、許可されていない場合にはデータを破棄して終了し、許可されている場合には対応する要件をセキュリティポリシーから抽出し、要件がセキュリティポリシー内に存在しない場合には文書の読み取りを行って終了し、要件がセキュリティポリシー内に存在する場合にはすべての要件を読み取る方法で実行可能であるかを判定し、実行可能でない要件が存在する場合にはデータを破棄して終了し、すべての要件を実行可能である場合には抽出された前記要件を満たして文書の読み取りを行って終了する、セキュリティポリシーに基づいて文書を読み取る方法により実現する。

【選択図】 図 1

特願 2002-297888

出 願 人 履 歴 情 報

識別番号

[000006747]

1. 変更年月日

1990年 8月24日

[変更理由]

新規登録

住 所

東京都大田区中馬込1丁目3番6号

氏 名

株式会社リコー

2. 変更年月日

2002年 5月17日

[変更理由]

住所変更

住 所

東京都大田区中馬込1丁目3番6号

氏 名

株式会社リコー